PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-031130

(43)Date of publication of application : 02.02.1999

(51)Int.Cl. G06F 15/00
G09C 1/00
H04L 9/32

(21)Application number : 09-184866

(22)Date of filing : 10.07.1997

(71)Applicant : FUJI XEROX CO LTD

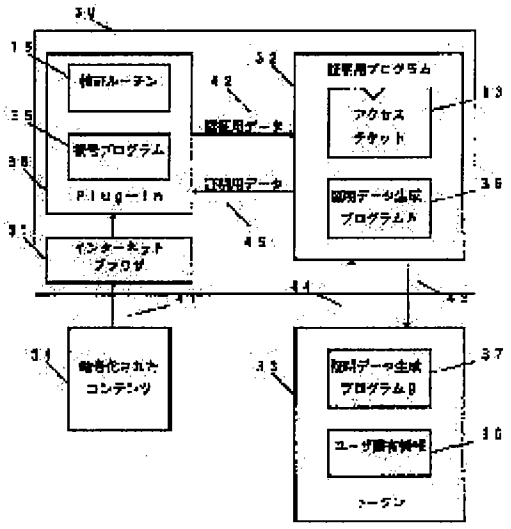
(72)Inventor : KONO KENJI
NAKAGAKI JUHEI
KOJIMA SHUNICHI

(54) SERVICE PROVIDING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide the utilization of service only to a user who has a legal right, minimizing the burden on the user and a service provider.

SOLUTION: When a plug-in 38 of an internet browser 31 is started, a verification program 15 in the plug-in 38 is started, communicates with a program 32 for certification and performs user authentication. A certification data generation program A36 of the program 32 cooperates with a certification data generation program B37 in a token 33, calculates based on a user inherent information 16 and an access ticket 13 and communicates with the program 15 in the plug-in 38 based on the calculation. As the result of the communication, the success of authentication by the program 15 is limited to only when the three of the user inherent information, the access ticket and enciphered contents correctly correspond with one another.



LEGAL STATUS

[Date of request for examination] 13.06.2002

[Date of sending the examiner's decision of rejection]	27.02.2007
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] In the service provision equipment which provides with service only the user who has a just right The 1st storage means which memorizes the data for authentication, and the 2nd storage means which memorizes a user's proper information, The 3rd storage means which memorizes the auxiliary information for certification which it is as a result of activation that predetermined count was performed, to said user's proper information, and the description information on access rating authentication, The data for authentication currently held at said 1st storage means, and said user's proper information memorized by said 2nd storage means, Service provision equipment characterized by offering service using the certification data which have a certification data generation means to perform predetermined count to said auxiliary information for certification memorized by said 3rd storage means, and to generate certification data, and were generated by said certification data generation means.
[Claim 2] In the service provision equipment which provides with service only the user who has a just right The 1st storage means which memorizes the data for authentication, and the 2nd storage means which memorizes a user's proper information, The 3rd storage means which memorizes the auxiliary information for certification which it is as a result of activation that predetermined count was performed, to said user's proper information, and the description information on access rating authentication, The data for authentication currently held at said 1st storage means, and said user's proper information memorized by said 2nd storage means, A certification data generation means to perform predetermined count to said auxiliary information for certification memorized by said 3rd storage means, and to generate certification data, It has a certification data verification means to verify that the certification data generated by said certification data generation means are generated based on the description information on said access rating authentication. Service provision equipment characterized by offering service only when verification by said certification data verification means is successful.
[Claim 3] Service provision equipment according to claim 2 characterized by canceling the limit of use to said information and enabling informational use only when it has further an input means to input the information which had use restricted and verification by said certification data verification means is successful.
[Claim 4] It is service provision equipment according to claim 2 or 3 which the description information on said access rating authentication is a decode key in an encryption function, and said data for authentication encipher suitable data using the encryption key corresponding to said decode key, and carries out [judging with verification being successful when, as for said certification data-verification means, the certification data which said certification data generation means generates decode said data for authentication correctly, and] as the description.
[Claim 5] It is service provision equipment according to claim 2 or 3 characterized by for the description information on said access rating authentication being an encryption key in an encryption function, and judging with verification having been successful when, as for said certification data verification means, the certification data which said certification data generation means generates enciphered said data for authentication correctly.

[Claim 6] It is service provision equipment according to claim 2 or 3 characterized by for the description information on said access rating authentication to be a signature key in a digital-signature function, and for said certification data-verification means to judge with verification having been successful when it was verified that the certification data which said certification data generation means generates are the digital signature correctly generated to said data for authentication using said signature key.
[Claim 7] The information which had said use restricted is service provision equipment according to claim 2 to 6 which is the information as which at least the part was enciphered, and is characterized by decoding said enciphered information and enabling informational use only when verification by said certification data verification means is successful.
[Claim 8] It has an input means to input the enciphered information, further, and the description information on said access rating authentication is the 1st decode key in an encryption function. Said data for authentication encipher the 2nd decode key which decodes said enciphered information using the encryption key corresponding to said 1st decode key. Service provision equipment according to claim 1 or 2 characterized by for the certification data generated by said certification data generation means being said 2nd decode key, decoding said enciphered information using said 2nd decode key, and offering the service corresponding to said information.
[Claim 9] Service provision equipment of a key according to claim 4, 5, or 8 with which said encryption function is an unsymmetrical key encryption function, and the description information on said access rating authentication comes out on the other hand, and it is characterized by a certain thing.
[Claim 10] Service provision equipment according to claim 4, 5, or 8 characterized by for said encryption function being a public-key-encryption-ized function and the description information on said access rating authentication being a private key.
[Claim 11] Service provision equipment according to claim 4, 5, or 8 characterized by for said encryption function being a symmetry key encryption function, and the description information on said access rating authentication being a common private key.
[Claim 12] In the service provision equipment which has access rating authentication equipment which certification data generation equipment and certification data verification equipment are provided, and said certification data generation equipment and said certification data verification equipment communicate, and attests a user's access rating 1st storage means by which said certification data generation equipment memorizes the data for authentication, The 2nd storage means which memorizes a user's proper information, and said user's proper information, The 3rd storage means which memorizes the auxiliary information for certification which it is as a result of activation that predetermined count was performed, to the description information on access rating authentication, Said data for authentication currently held at said 1st storage means, and said user's proper information currently held at said 2nd storage means, It has a certification data generation means to perform predetermined count to said auxiliary information for certification currently held at said 3rd storage means, and to generate certification information. Said certification data verification equipment The 4th storage means which memorizes the data for authentication, and the 5th storage means which memorizes certification data, It has a certification data verification means to verify that said certification data generated by said certification data generation means are generated based on the description information for said access rating authentication. Said certification data verification equipment writes out said data for authentication memorized by said 4th storage means to said 1st storage means of said certification data generation equipment. Said certification data generation equipment Said certification data generated based on said data for authentication written in said 1st storage means by said certification data generation means It is service provision equipment which writes out to said 5th storage means of said certification data verification equipment, and is characterized by said certification data verification equipment attesting a user's access rating using said certification data written in said 5th storage means.
[Claim 13] The description information for said access rating authentication is the decode key of an encryption function. Said certification data verification equipment A random-number generation means, While it has the 6th storage means which memorizes the generated random number, and the 7th storage means which memorizes the ** data for authentication and said random-number generation means

writes the generated random number in said 6th storage means After giving the random-number effectiveness which used said random number for said ** data for authentication memorized by said 7th storage means, It writes in said 4th storage means as said data for authentication. Said certification data verification means The result of having removed the random-number effectiveness by said random number memorized by said 6th storage means from said certification data in which it was written by said 5th storage means with said certification data generation equipment Service provision equipment according to claim 12 characterized by verifying decoding said ** data for authentication memorized by said 7th storage means with the decode key which is the description information on said access rating authentication.

[Claim 14] The description information for said access rating authentication is the encryption key of an encryption function. Said certification data verification equipment is equipped with a random-number generation means, and said random-number generation means is written in said 4th storage means by using the generated random number as said data for authentication. Said certification data verification means Service provision equipment according to claim 12 with which said certification data written in said 5th storage means by said certification data generation equipment are characterized by verifying decoding said random number.

[Claim 15] The description information for said access rating authentication is the signature key of a digital signature function. Said certification data verification equipment is equipped with a random-number generation means, and said random-number generation means is written in said 4th storage means by using the generated random number as the data for authentication. Said certification data verification means Said certification data written in said 5th storage means by said certification data generation equipment Service provision equipment according to claim 12 characterized by verifying that it is a digital signature with the signature key which is the description information on said access rating authentication to the data for authentication which are said random number.

[Claim 16] Service provision equipment according to claim 1 to 15 with which said 2nd storage means and said certification data generation means are characterized by being saved in a defense means to close observing an in-house data and processing procedure from the outside if at least.

[Claim 17] Service provision equipment according to claim 1 to 15 characterized by constituting said 2nd storage means and said certification data generation means as a portable small arithmetic unit of an IC card etc. at least.

[Claim 18] Service provision equipment according to claim 1 to 15 with which said certification data verification means is characterized by being saved in a defense means to close observing an in-house data and processing procedure from the outside if at least.

[Claim 19] Service provision equipment according to claim 1 to 15 characterized by constituting said certification data verification means as a portable small arithmetic unit of an IC card etc. at least.

[Claim 20] It is service provision equipment according to claim 1 to 19 which the information inputted from said input means enciphers multimedia information or said multimedia, such as an image, an animation, voice, and music, and is characterized by said service reproducing said inputted information.

[Claim 21] Said auxiliary information for certification which has further the 8th storage means which memorizes the use control information which controls generation of said certification data, and is held at said 3rd storage means It is as a result of [of having performed predetermined count to said user's proper information, the description information on said access rating authentication, and said use control information] activation. Said certification data generation means The data for authentication currently held at said 1st storage means, and said user's proper information memorized by said 2nd storage means, Service provision equipment according to claim 1 to 20 characterized by performing predetermined count to said auxiliary information for certification memorized by said 3rd storage means, and said use control information memorized by said 8th storage means, and generating certification data.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the service provision equipment which can provide with service alternatively only the user who has a just right, and its approach.
[0002]
[Description of the Prior Art] The time which various information is digitized by development of a network in recent years, and circulates through a network by it has come. As information digitized, there are an end still picture, an animation, voice, a program, etc. about text, and we can receive various services which combined these on the network. However, the ease of the copy which is the big description of these digital information had become the factor which checks circulation of the digital information in a network until now. Since this can generate the completely same object as original if digital information is copied, what once circulated is used without notice in the place which an author does not mean, and it originates in the problem of being hard to collect the just countervalues which an author should get.
[0003] In order to solve this problem, recently, encipher digital information and it is made to circulate freely like CD-SHOWCASE (a trademark or product name) of IBM Japan Corp., and in case it uses, price is paid and a system which uses reception and digital information for a decode key by the telephone line etc. has also appeared. Moreover, the example of the system which charges according to the amount using software and collects tariffs is shown in the "software management method" of JP,6-95302,B. The amount measuring device of information use which can measure exactly the amounts of use, such as information utilization time of all the users of the information distributed by broadcast, is described by the "amount measuring device of information use" of JP,7-21276,B. According to this, the amount measuring device of information use receives and accumulates the enciphered books information, and the example for which the user records the time amount and the amount which decoded and displayed books information as use hysteresis, and collects a tariff by that cause is shown.
[0004] Various code techniques as an approach and the program execution control technique of realizing the aforementioned system are known as advanced technology.
[0005] The user who has tried activation of application inspects holding the key for authentication of normal, ** this routine is restricted when existence of the key for the ** aforementioned authentication is checked, a program execution control technique embeds the routine for a user's access rating authentication into ** application program, and it continues a program, and when other, it is the technique which stops program execution. By using this technique, if only the user of the normal which holds an authentication key is possible, he can close activation of application. It is put in practical use in the software **** enterprise and this technique is RainbowTechnologies as a product, for example. Sentinel of an Inc. company SuperPro (trademark) and Aladdin Knowledge Systems There is an HASP (trademark) of a Ltd. company etc.
[0006] A program execution control technique is explained more below at a detail.
** The user who performs software holds an authentication key as user proper information. An

authentication key is a key for encryption and those who permit use of software, for example, a software vendor, distribute it to a user. An authentication key is severely enclosed with the memory in hardware, in order to prevent a duplicate, and it is delivered by the user using a postal physical means.
** Equip an owner's personal computer or workstation by the approach which had the hardware which built in the user authentication key specified. A printer port etc. is equipped with hardware.
** If a user starts an application program and program execution attains to said access rating authentication routine, a program will communicate with the hardware which built in a user's authentication key. If a program identifies an authentication key and existence of a right authentication key is checked based on a communication link result, activation will be moved to the following step. When a communication link goes wrong and existence of an authentication key is not checked, a program stops oneself and can be made not to perform subsequent activation.
[0007] Discernment of the authentication key by the access rating authentication routine is performed by the following protocols, for example.
** An access rating authentication routine generates a suitable number, and transmits to hardware with a built-in key.
** The hardware with a built-in key enciphers the number sent using the authentication key to build in, and answers said access rating authentication routine.
** An authentication routine judges whether it is the number with which the answered number enciphers the number expected beforehand, i.e., the number transmitted to hardware, with a right authentication key, and is obtained.
** It continues program execution, in being in agreement with the number with which the number with which a letter was answered was expected, and in not being in agreement, it stops a program.
[0008] Even if the application program in this case and the communication link between hardware with a built-in authentication key are exchanged between the same hardware in the same part in the same application program, they must differ at every activation. Otherwise, it will also enable the user who does not hold a right authentication key to perform a program by answering an application program in the contents of a communication link which recorded the contents of a communication link in a normal activation process once, and were recorded whenever it performed the program after that. Such an attack is called a replay attack.
[0009] In order to prevent a replay attack, the number usually sent to hardware with a built-in key uses the random number newly generated at every communication link.
[0010] The trouble of the [trouble of conventional technique] conventional technique originates in the property in which protection processing of a program must be performed based on this authentication key, after a programmer assumes beforehand the authentication key which a user has, when creating an application program.
[0011] That is, only when the right reply from hardware with a built-in key is beforehand carried out a side at the time of a programming and a right reply is received, the implementer of a program has to create a program so that a program may be performed normally.
[0012] Although the use gestalt of the conventional technique of having the aforementioned description becomes the two aforementioned kinds fundamentally, it has the problem which states below in any case.
[0013] ** By the 1st approach, prepare a user's authentication key so that it may differ for every user. That is, every one different authentication key for every user is prepared for the user first like authentication **** at authentication **** and the user second. In this case, the authentication routine in a program must be created so that the authentication key of the proper of the user using this program can be attested, and a programmer needs to create the program from which only the number of use users differs.
[0014] When the target users are a large number, the activity which customizes a program for every user (individualization) requires an effort intolerable for a programmer, and becomes what also has a huge list of user authentication keys which must be managed.
[0015] ** By the 2nd approach, the implementer of a program prepares an authentication key which is

different for every application, respectively. That is, every one authentication key which is different for every application like authentication **** is prepared for the application first at authentication **** and the application second, and each application program is created so that the authentication key of a proper may be identified.
[0016] Although it becomes unnecessary to create a program individually for every user like the 1st approach by this approach, as for a user, only the number of the applications to be used must hold an authentication key conversely.
[0017] As mentioned above, it is necessary to distribute an authentication key to a user in the condition of having enclosed with hardware severely. Therefore, it cannot but depend for distribution of the hardware which builds in an authentication key on a postal physical means to the ability to distribute the program itself simple through a network. the hardware with which the authentication key corresponding to [to whenever / upper ****** / in a programmer] the application for since [use consent / of the application from a user] was enclosed -- it is necessary to mail -- cost, time amount, and the time and effort of packing -- it becomes a very big burden for a programmer about any.
[0018] Moreover, a user must be content with the complicatedness that hardware must be exchanged whenever it changes the application to be used.
[0019] Though he wants to use application with a user, it must wait until the hardware with which the authentication key was enclosed is mailed and it arrives, and there is also a problem that it cannot use immediately.
[0020] Although the approach of teaching a user the password for making the authentication key in hardware available whenever it encloses two or more authentication keys beforehand into hardware and permits a user use of new application can be used in order to mitigate these problems, when the authentication key enclosed beforehand is exhausted, the same problem occurs, and it has not become essential solution.
[0021] You may consider that it is hardly defended since a user can copy application so that he may like, once it decodes application by this approach, although the simple method of only enciphering application in addition to the approach of the above effective control, and teaching a user that decode key by the safe approach is used generally and widely, and it can distribute unjustly.
[0022] Therefore, when the digitized information, for example, software, music, a movie, etc. tended to be delivered in a network (these are henceforth called contents generically) and it was going to obtain a just countervalue, in a Prior art, there was a problem of management of contents becoming complicated or applying a big burden to a user by management of the hardware for authentication.
[0023]
[Problem(s) to be Solved by the Invention] This invention aims at offering the system which can provide with use of service only the user who has a just right, or the system which can collect the just countervalues according to use of service, being made in view of such a problem and pressing down the burden of a user and a service provider to the minimum.
[0024]
[Means for Solving the Problem] The 1st storage means which memorizes the data for authentication to the service provision equipment which provides with service only the user who has a just right in order to attain the above-mentioned purpose according to the 1st side face of this invention, The 2nd storage means which memorizes a user's proper information, and said user's proper information, The 3rd storage means which memorizes the auxiliary information for certification which it is as a result of activation that predetermined count was performed, to the description information on access rating authentication, The data for authentication currently held at said 1st storage means, and said user's proper information memorized by said 2nd storage means, He is trying to establish a certification data generation means to perform predetermined count to said auxiliary information for certification memorized by said 3rd storage means, and to generate certification data.
[0025] Moreover, the 1st storage means which memorizes the data for authentication to the service provision equipment which provides with service only the user who has a just right according to the 2nd side face of this invention, The 2nd storage means which memorizes a user's proper information, and

said user's proper information, The 3rd storage means which memorizes the auxiliary information for certification which it is as a result of activation that predetermined count was performed, to the description information on access rating authentication, The data for authentication currently held at said 1st storage means, and said user's proper information memorized by said 2nd storage means, A certification data generation means to perform predetermined count to said auxiliary information for certification memorized by said 3rd storage means, and to generate certification data, He is trying to establish a certification data verification means to verify that the certification data generated by said certification data generation means are generated based on the description information on said access rating authentication.

[0026] According to these configurations, by introducing the auxiliary data for certification (access ticket) The description information for access rating authentication which is a protection side and is given, and the user proper information given to a user side can be made to become independent. A user possesses user proper information beforehand and protection persons, such as a programmer, create an application program using the description information on access rating authentication independently of the user proper information which a user possesses. Then, by creating and distributing an access ticket according to a user's **** information and the description information on the access ticket rating authentication used for creation of an application program etc. It becomes possible to attest user access ratings, such as execution control, and only the user who has a just right can be provided with desired service. Moreover, if a log is taken to a certification data generate time, the just countervalue to service is recoverable.

[0027] Moreover, you may make it held in the aforementioned configuration in a defense means to close if it is difficult for said 2nd storage means and said certification data generation means to observe an in-house data and processing procedure from the outside at least.

[0028] Moreover, you may make it held in the aforementioned configuration in a defense means to close if it is difficult for said certification data verification means to observe an in-house data and processing procedure from the outside at least.

[0029] Moreover, the description information on said access rating authentication is a decode key in an encryption function, and data with said suitable data for authentication are enciphered using the encryption key corresponding to said decode key, and you may make it verify that the certification data which said certification data generation means generates decode said data for authentication correctly with said certification data verification means. Moreover, the description information on said access rating authentication is an encryption key in an encryption function, and said data for authentication decode suitable data using the decode key corresponding to said encryption key, and you may make it verify that the certification data which said certification data generation means generates encipher said data for authentication correctly with said certification data verification means. Moreover, you may make it verify that the certification data which the description information on said access rating authentication is a signature key in a digital signature function, and said certification data generation means generates are the digital signature correctly generated to said data for authentication using said signature key.

[0030] Moreover, the description information on said access rating authentication is the 1st decode key in an encryption function. Said data for authentication encipher the 2nd decode key which decodes said enciphered information using the encryption key corresponding to said 1st decode key. The certification data generated by said certification data generation means are said 2nd decode key, and said enciphered information is decoded using said 2nd decode key, and you may make it offer the service corresponding to said information. Moreover, said encryption function may be an unsymmetrical key encryption function, and the description information on access rating authentication may be one side of a key.

[0031] Moreover, said encryption function may be a public-key-encryption-ized function and the description information on access rating authentication may be a private key.

[0032] Moreover, said encryption function may be a symmetry key encryption function, and the description information on access rating authentication may be a common private key.

[0033] Moreover, said 1st storage means, said 2nd storage means, and said 3rd storage means, The

certification data generation equipment which consists of said certification data generation means, and the 4th storage means which memorizes the data for authentication in addition to said certification data verification means, In the service provision equipment which has access rating authentication equipment with which the certification data verification equipment which offered the 5th storage means which memorizes certification data attests a user's access rating by communicating mutually Certification data verification equipment writes out the data for authentication memorized by the 4th storage means to the 1st storage means of certification data generation equipment. Certification data generation equipment The certification data generated based on said data for authentication written in the 1st storage means by the certification data generation means It rakes out for the 5th storage means in certification data verification equipment, and certification data verification equipment can attest a user's access rating using said certification data written in the 5th storage means.

[0034] The description information for access rating authentication is the decode key of an encryption function. Certification data verification equipment Moreover, a random-number generation means, While it has the 6th storage means which memorizes the generated random number, and the 7th storage means which memorizes the ** data for authentication and a random-number generation means writes the generated random number in the 6th storage means After giving the random-number effectiveness which used said random number for the ** data for authentication memorized by the 7th storage means, it writes in the 4th storage means as data for authentication. A certification data verification means The result of having removed the random-number effectiveness by the random number memorized by the 6th storage means from the certification data in which it was written by the 5th storage means with said certification data generation equipment You may make it verify decoding the ** data for authentication memorized by the 7th storage means with the decode key which is the description information on access rating authentication.

[0035] Moreover, the description information for access rating authentication is the encryption key of an encryption function, and certification data-verification equipment is equipped with a random-number generation means, a random-number generation means writes in the 4th storage means by using the generated random number as the data for authentication, and it may make it verify that the certification data written in the 5th storage means by certification data generation equipment decode said random number in a certification data-verification means.

[0036] Moreover, the description information for access rating authentication is the signature key of a digital signature function. Certification data verification equipment is equipped with a random-number generation means, and a random-number generation means is written in the 4th storage means by using the generated random number as the data for authentication. A certification data verification means You may make it verify that the certification data written in the 5th storage means by certification data generation equipment are a digital signature with the signature key it is [key] the description information on access rating authentication to the data for authentication which are said random number.

[0037]

[The mode of implementation of invention] Hereafter, this invention is explained to a detail.

[Example 1] With reference to an example 1, the theoretic configuration of this invention is explained first. Drawing 1 shows the configuration of the example 1 of this invention as a whole, the service provision system consists of certification data verification equipment 10 and certification data generation equipment 11 in this drawing 1 , and certification data generation equipment 11 receives the access ticket (auxiliary data for certification) 13 from access ticket generation equipment 12. Certification data verification equipment 10 performs the verification routine 15. Certification data generation equipment 11 holds the user proper information 16 and the access ticket 13, and performs the certification data generator 17. A part of user proper information 16 and certification data generator [at least] 17 are protected with tamper-proof equipment 20.

[0038] Access ticket generation equipment 12 generates the access ticket 13 based on the description information 14 on access rating authentication, and a user's proper information 16, and the access ticket 13 is sent to a user through a network, a storage, etc., and is held at a user's certification data generation

equipment 11.
[0039] Certification data verification equipment 10 transmits the data 18 for authentication to certification data generation equipment 11. Certification data generation equipment 11 generates the certification data 19 using the access ticket 13 and the user proper information 16, and answers certification data verification equipment 10 in this. Certification data verification equipment 10 verifies the justification of certification data based on the data for authentication. That is, it verifies that certification data are data generated based on the data for verification, and the description information on access rating authentication.
[0040] If the justification of certification data is verified, it will be attested that a user has a just right and desired service will be offered by service provision equipment.
[0041] Hereafter, taking the case of actual service, this invention is concretely explained using drawing 2 .
[0042] The example 1 of this invention describes the example which unified the certification data verification routine 15 and the decode program 35, and was included in the Internet browsers (trademark - of Netscape Navigator-U.S. Netscape Communications, Inc. etc.) as a plug-in (Plug-In) module. Here, a plug-in module can point out the software program which extends the function of the Internet browser, and, thereby, use of a new data type can be supported to a user. If the information on the data type which the Internet browser is not supporting is received from a server, the Internet browser will be loaded and started in search of plug-in related with the data type. Thereby, the support of a new data type is enabled seamlessly, without changing a user's existing system.
[0043] The contents 34 enciphered as the new data type in the case of this example are pointed out, and if the contents 34 as which the Internet browser was enciphered are received from a server, the Internet browser will look at the data type of the enciphered contents 34, and will be loaded and started in search of the plug-in 38 related with the data type. Started plug-in starts the verification routine 15, and verifies by using for the program 32 for certification delivery and the certification data to which it came on the contrary for the data for authentication. When verification is successful with the verification routine 15, the enciphered contents 34 are decoded by the decode program 35, and it is provided for a user by it. The decoded contents are information, the downloaded programs, such as a hyper-document, an image, an animation, and music.
[0044] Certification data generation equipment consists of a program 32 for certification, and a token 33. The program 32 for authentication is a software program containing the access ticket 13 and the authentication data generator A36, and operates on a user's personal computer (PC). As for a token 33, it is desirable to constitute including the authentication data generator B37 and the user proper information 16 by the hardware (for it to be hereafter called the Tampa-proof hardware) which has the defense force to theft of the internal state by the probe. Because, user **** information is equivalent to the password in password authentication, and it is the important only information that a user's identity is proved, and when the user proper information 16 can be read, copied and distributed, a person without a just right will be allowed unjust use of contents.
[0045] Moreover, in addition to said user proper information, the certification data generators A and B which perform predetermined count procedure are given to a user. This program is for communicating with the verification routine 15 in plug-in 38, and if the user proper information 16 and the access ticket 13 are given, it will generate the certification data 45 which calculate to the data 42 for authentication and prove a user's identity. Although the user proper information 16 is used in process of this count, since there is a problem when the user proper information 16 is revealed outside for the reason mentioned above, the certification data generator B37 using user proper information is stored in said Tampa-proof hardware. IC chip protected by the IC card, resin mold, etc. is simple, and it is easy to apply it as Tampa-proof hardware. However, when the added value of the service to offer is very high, the equipment which has high safety as shown with "the encryption equipment, the decode equipment, the secret data processor, and information processor" of Japanese Patent Application No. No. 284475 [08 to] may be used.
[0046] Several operations of the certification data verification routine 15 are described below.

[0047] 1. Into the certification data verification routine 15, the reply data (expected value) it is expected that are data (data 42 for authentication) which should be transmitted are embedded. The certification data verification routine 15 takes out said transmit data, transmits to a user, and receives a reply from a user. Subsequently, when the reply data and said expected value from a user are compared and both are in agreement, the contents 34 enciphered by the decode program 35 are decoded, and a user is provided with contents in the available condition.
[0048] 2. Into the certification data verification routine 15, the reply data (expected value) it is expected that are data which should be transmitted are embedded. The certification data verification routine 15 takes out said transmit data, transmits to a user, and receives a reply from a user. Subsequently, the contents 34 enciphered by the decode program 35 in the value which gave the tropism function from the user to reply data on the other hand when both were in agreement as compared with said expected value are decoded, and a user is provided with contents in the available condition.
[0049] It sets to an operation of the above 1 and 2, and in being as a result of the encryption to which reply data follow the predetermined encryption algorithm of transmit data, the description information on access rating authentication serves as an encryption key. Moreover, in [reply data] being a digital signature according to the predetermined signature algorithm of transmit data, the description information on access rating authentication serves as a signature key.
[0050] 3. The data which should be transmitted are embedded into the certification data verification routine 15. The certification data verification routine 15 takes out said transmit data, transmits to a user, and receives a reply from a user. Subsequently, the contents 34 enciphered by the decode program 35 are decoded by using said reply data as a decode key, and a user is provided with contents in the available condition.
[0051] 4. The data which should be transmitted are embedded into the certification data verification routine 15. After the certification data verification routine 15 takes out said transmit data and gives the random-number effectiveness, it transmits to a user, and it receives a reply from a user. Subsequently, the contents 34 enciphered by the decode program 35 are decoded by using as a decode key the result of having removed said random-number effectiveness from said reply data, and a user is provided with contents in the available condition.
[0052] 5. The certification data verification routine 15 receives the transmit data corresponding to the enciphered contents. In this case, the transmit data may be embedded in the enciphered contents. The certification data verification routine 15 transmits said received transmit data to a user, and receives a reply from a user. Subsequently, the contents 34 enciphered by the decode program 35 are decoded by using said reply data as a decode key, and a user is provided with contents in the available condition.
[0053] 6. The certification data verification routine 15 receives the transmit data corresponding to the enciphered contents. In this case, the transmit data may be embedded in the enciphered contents. The certification data verification routine 15 transmits to a user, after giving the random-number effectiveness to said received transmit data, and it receives a reply from a user. Subsequently, the contents 34 enciphered by the decode program 35 are decoded by using as a decode key the result of having removed said random-number effectiveness from said reply data, and a user is provided with contents in the available condition.
[0054] In the above 3 thru/or an operation of 6, when a right decode key is obtained from reply data, the contents 34 as which the hook was enciphered are decoded correctly, and a user becomes available about these contents. The description information on the access rating authentication in this case serves as a decode key for decoding the enciphered decode key.
[0055] Now, with the execution control technique stated in the conventional example, user proper information (a user's authentication key) is the same as the description information on access rating authentication. The conventional certification data generating routine calculates reply data by inputting the description information on access rating authentication, and the data transmitted from the certification data verification routine.
[0056] On the other hand, the user proper information 16 and the description information 14 on access rating authentication have the description of this invention in a mutually-independent point. In addition

to the data 42 transmitted from the user proper information 16 and the certification data verification routine 15, the certification data generators A and B calculate the reply data (certification data) 45 also for this configuration by considering the access ticket 13 as an input. This configuration has the following properties.

[0057] 1. The access ticket 13 is data calculated based on the specific user proper information 16 and the description information 14 on access rating authentication.

2. It is impossible in computational complexity at least to calculate the description information 14 on access rating authentication for the user proper information 16 from the access ticket 13 to not knowing.

3. The certification data generators A and B calculate right reply data only within the case where the right combination of the user proper information 16 and the access ticket 13 is inputted, when the user proper information 16 and the access ticket 13 are right combination.

[0058] By the above, a user can possess the user proper information 16 beforehand, a contents implementer can encipher contents independently [the user proper information 16 which a user possesses], and the user proper information 16 can enjoy use of the contents enciphered independently only to the user who has a just right by creating the access ticket 13 according to the user proper information 16 and the description information on access rating authentication.

[0059] Moreover, the proper information which shall consist of two proper information and uses the user proper information 16 on the occasion of creation of the access ticket 13, and the proper information which a user uses in a communications program can also be distinguished and used. The most typical example is the approach of making user proper information 16 a public key pair, using for access ticket creation by making a public key into open proper information, and enclosing the private key in the token 33 as a user individual's secret proper information. In this case, by enabling it to calculate the access ticket 13 from the description information 14 on access rating authentication, and the public key of said public key pair, it becomes possible to calculate the access ticket 13, keeping secret the user proper information 16 which is a private key.

[0060] Next, a more concrete configuration is **(ed) and explained to an example. In drawing 2 , the Internet browser 31, plug-in 38, and the program 32 for certification are realizable as a software program on the computer 30 (PC or workstation) which a user uses. Although you may realize as a software program similarly about a token 33, in order to raise the safety of the proper information (user proper information) for identifying a user, it is desirable to use together the tokens 33 (an IC card, a PC card, board, etc.) which have the Tampa-proof property connected to this computer 30. Under the present circumstances, if the hardware which has portability like an IC card is used, it is convenient when a user works on two or more PCs or a workstation.

[0061] The enciphered contents 34 which are used by the Internet browser 31 are supplied to a user using storages, such as a network, CD-ROM, DVD, and a floppy disk.

[0062] If a user demands use of the contents enciphered from the Internet browser, the Internet browser will look at the data type of the enciphered contents, and will load and start it in search of plug-in related with the data type.

[0063] If plug-in starts, the verification program in this plug-in starts, it will communicate with the program 32 for certification, user authentication will be performed, and decode of these contents will be performed only within the case where a communication link is completed correctly.

[0064] In order to use the contents 34 as which the user was enciphered, it is necessary to acquire the access ticket (auxiliary information for certification) published by user him. A user equips said PC or workstation with an IC card, when user proper information is enclosed with the IC card, for example, while registering the acquired access ticket into the program 32 for certification installed on said PC or the workstation.

[0065] In harmony with certification data generator B, certification data generator A calculates based on the user proper information 16 and the access ticket 13, and performs the verification program 15 and communication link in plug-in based on the count.

[0066] As a result of a communication link, when [with the contents enciphered as user proper information and an access ticket] three correspond surely, it restricts that authentication by the

verification program 15 is successful. Authentication is not successful when either user proper information or an access ticket is missing.
[0067] An access ticket is published by specific addressing to a user. That is, a specific user's user proper information is used on the occasion of generation of an access ticket. When the user proper information used for an access ticket generate time and said user proper information used by the certification data generator are not in agreement, authentication is not successful too.
[0068] Moreover, an access ticket is generated based on the description information on specific access rating authentication, and the verification program 15 is constituted so that the description information on this access rating authentication may be attested. Therefore, authentication is not successful also when the description information used as the basis of generation of an access ticket and the description information which the verification program 15 tends to attest do not correspond mutually.
[0069] Since it has safety sufficient in itself, an access ticket can be delivered through a network. The safeties of an access ticket are the following two properties.
[0070] 1. the user by whom an access ticket is a registered form and the access ticket was published -- only he (holder of the user proper information that it was correctly used for the access ticket generate time) can operate certification data generation equipment correctly using this access ticket. Therefore, even if a holder in bad faith intercepts a network and gets other users' access ticket unjustly, unless this third person gets the user proper information on the normal which is the issue place of an access ticket, it is impossible to use this access ticket.
[0071] 2. The access ticket holds still stricter safety. That is, even if a holder in bad faith collects the access tickets of the number of arbitration and performs what kind of analysis, it is impossible to constitute equipment which another access ticket is forged [equipment] based on the acquired information, or actuation of certification data generation equipment is copied [equipment], and forms authentication.
[0072] In the example 1, the access ticket t is data generated based on the following formula 1.
[0073]
[Equation 1]
(1) T=D-e+omegaphi (n)
All the notations in an upper type are integers, and express the following. n -- RSA (Rivest-Shamir-Adelman) -- law -- it is the product of a number p and q, i.e., the two sufficiently big prime factors, (n=pq). phi (n) is the Euler number of n, i.e., the product of p-1 and q-1, (phi (n) = (p-1) (q-1)). e expresses user proper information, it is a different number for every user, and it uses it in order to identify a user. D -- an access ticket private key, i.e., the description information on access rating authentication, -- expressing -- law -- it is a RSA private key under a number n, and a formula 2 is filled.

[0074]
[Equation 2] (2) gcd(D, phi (n)) =1 -- here, gcd (x y) expresses the greatest common measure of more than 2 [x] and y. The property expressed by the formula (2) guarantees that several E which fills a formula 3 exists.
[0075]
[Equation 3] (3) ED mod phi(n) =1E is called an access ticket public key.
[0076] omega is a number which becomes settled depending on n and e, and when n differs either from e, its value of the corresponds easily, twists it (it does not collide), and it is defined like. There is also a method of omega setting and on the other hand defining omega like a formula 4 as an example of the direction using tropism Hash Function h.
[0077]
[Equation 4] (4) Omega=h (n|e)
However, notation | expresses association of a bit string.
[0078] On the other hand, tropism Hash Functions are x which fills h(x) =h (y) and which is different from each other, and a function in which computing y has the property in which it is remarkable and difficult. On the other hand, it is RSA as an example of a tropism Hash Function. Data Security MD2

and MD4 by Inc., MD5, and the specification SHS (Secure Hash Standard) by the U.S. federal government are known.
[0079] In the number which appeared during the above-mentioned explanation, t, E, and n can be exhibited and D, e, omega, p, remaining q, and remaining phi (n) need to be secret in addition to those who have the right which creates a ticket.
[0080] The schematic diagram of the computer (PC or workstation) which a user uses for drawing 3 is shown. In drawing 3 , the card reader 39 is connected to the computer 30 which a user uses, and a user inserts and uses a token 33 for a card reader 39. The Internet browser 31, plug-in, and the program for certification are realized as a software program on a computer 30. Moreover, the access ticket is also memorized in the storage region of a computer 30. Now, the contents which it is going to use are the images of the picture of a yacht, and if a user with a just token and a just access ticket makes the enciphered contents read into the Internet browser 31, as shown in drawing 3 , the image of the picture of a yacht will be displayed on the Internet browser 31 by plug-in.
[0081] With reference to drawing 4 , an example 1 is further explained to a detail. Drawing 4 shows concretely the example of a configuration of the example 1 of this invention. If it is made to contrast with drawing 2 , the thing corresponding to the verification routine 15 consists of the access ticket public key storage section 51, the authentication data storage section 52, the random-number-generation section 53, the random-number storage section 54, the transmit data (challenge) count section 55, the data separation section 56, a certification data receive section 57, the random-number effectiveness removal section 58, and the verification section 59, and the decode program 35 runs on decode / display 61. Although a verification routine and a decode program are divided and being constituted from this example, a decode program may be made merged to a verification routine if needed. Moreover, the program 32 for certification consists of the data receive section 71 for authentication, the access ticket storage section 72, the 1st operation part 73, and the certification data generation section 76, and a token 33 consists of the user proper information storage section 74 and the 2nd operation part 75.
[0082] Next, actuation is explained. All the variables in the following explanation are integers.
[0083] [Step 1]: If a user demands use of the contents enciphered from the Internet browser, the Internet browser will look at the data type of the enciphered contents, and will load and start it in search of plug-in related with the data type. If corresponding plug-in starts, the verification routine 15 in plug-in will start. The contents in this case point out what a user uses through the Internet browser, for example, it is the display information on a homepage (an image, an animation, hyper-document, etc.), or they are programs like a Java applet.
[0084] [Step 2]: The verification routine 15 of plug-in takes out an access ticket public key (E, n) and the authentication data KE from the contents enciphered in the data separation section, and stores them in the access ticket public key storage section 51 and the authentication data storage section 52, respectively. Here, this access ticket public key and these authentication data were explained as what is distributed along with the enciphered contents. Thus, it is desirable to accompany the contents enciphered as this access ticket public key and these authentication data consider safety although they may accompany the enciphered contents and you may enable it to come to hand through a network, and, as for these authentication data, being embedded so that a user may not understand is still more desirable. For example, what is necessary is to encipher, to embed these authentication data into contents, and just to take the approach of decoding with the decode key given to plug-in, after taking out.
[0085] [Step 3]:, next the verification routine 15 generate a random number r in the random-number generation section 53, store it in the random-number storage section 54, and calculate transmit data (challenge) C according to a formula 5 using an access ticket public key (E, n), the authentication data KE, and a random number r.
[0086]
[Equation 5] (5) C=rEKE mod The n challenge C and the number n of access ticket public key methods (the number of the RSA methods) are transmitted to a certification data generation side. Since the random number r is contained in the value of C, it becomes a value which is different whenever it is a

communication link, and has the effectiveness of preventing a replay attack.
[0087] [Step 4]: In the program for certification, receive Challenge C and the number n of the RSA methods which were sent from the verification routine in the data receive section for authentication, and it is the following, and make and generate the certification data (response) R. First, in the 1st operation part, the access ticket t which uses the number n of the RSA methods as a key, and corresponds is acquired, under the number n of the RSA methods, a formula 6 is performed and middle information R' is obtained from the access ticket storage section 72.
[0088]
[Equation 6] (6) R'=Ct mod n[step 5]: -- the user proper information e that the 2nd operation part 75 is memorized by the user proper information storage section 74 -- acquiring -- a formula 7 -- performing -- difference -- Information S is acquired.
[0089]
[Equation 7] (7) S=Ce mod n[step 6]: and the certification data generation section 76 -- middle information [from the 1st and 2nd operation part 73 and 75] R', and difference -- Information S is acquired, a formula 8 is calculated and the certification data R are obtained.
[0090]
[Equation 8] (8) R=R'S mod n certification data R are transmitted to a verification routine.
[0091] [Step 7]: The random-number effectiveness removal section 58 of the verification routine 15 acquires the certification data R received in the certification data receive section 57, calculates a formula 9 with the random number r memorized by the random-number storage section 54, and obtains K'.
[0092]
[Equation 9] (9) K -- verify that 'K calculated in said random-number effectiveness removal section 58 in the =Rr-1 mod n [step 8]:verification section 59' is generated based on D which is the description information on access rating authentication. K'=K should be realized when K' is generated based on D which is the description information on access rating authentication surely. Whether this formula is realized has the approach of judging whether the data enciphered using this K' being decoded and it decoding correctly, the approach of judging by whether redundancy is given to K, the specific value is given to that part, and K' has that specific value, etc. Approaches, such as an international standard ISO 9796, can be used for the latter approach. Here, using the latter approach, explanation is continued on the assumption that it verifies.
[0093] [Step 9]: If verification in the verification section 59 is judged to be the right, a verification routine will pass decode key K' to decode / display 61.
[0094] [Step 10]: Decode / display 61 decodes and displays the enciphered contents which separated decode key K' from the verification section 59 in reception and the data separation section 56. It is more desirable for plug-in to display directly on the field which the Internet browser specified from the field of safety, since the decoded information may be copied by the Internet browser, although the approach of passing the decoded contents to the Internet browser and displaying by the Internet browser is also possible.
[0095] Thus, the user who has a just right can use the contents enciphered using the Internet browser. At this time, the decoded contents do not exist on temporary memory, but unjust use of the decoded contents can be prevented by making it disappear, after use of a user finishes.
[0096] By this example, the enciphered contents explained an access ticket public key (E, n) and the authentication data KE as what is accompanied and distributed. The example of a configuration of these enciphered contents is shown in drawing 5 . As shown in drawing 5 , the enciphered contents consist of contents bodies enciphered as an access ticket public key (E, n) and the authentication data KE. The data separation section of a verification routine reads these, and divides them into each part.
[0097] After the contents body is enciphered with Key K and verification is correctly completed using the authentication data KE, Key K can be restored through the random-number effectiveness removal section, and it becomes possible to decode a contents body using this key K.
[0098] In order to raise safety more, it is desirable to be embedded so that the authentication data KE cannot separate into a user easily. The one approach of this implementation is shown in drawing 6 .

Although the enciphered contents consist of contents bodies enciphered as an access ticket public key (E, n) and the authentication data KE like drawing 5 at drawing 6 , not only a contents body but the authentication data KE are enciphered further. Drawing 6 showed the authentication data KE as what is enciphered with Key Kp.

[0099] The data separation section of a verification routine holds the decode key Kp corresponding to this cryptographic key key KP (the example using a common key encryptosystem), decodes the authentication data enciphered using the decode key KP which separated the contents body enciphered as the authentication data KE enciphered as the access ticket public key (E, n), and is held from the inputted whole contents, and takes out authentication data KE. Then, after verifying using this authentication data KE and completing verification correctly, Key K can be restored through the random-number effectiveness removal section, and it becomes possible to decode a contents body using this key K.

[0100] Although encryption and a decryption showed Key K and Key KP as an example using the same key since the example which used the common key encryption system here although a contents body and authentication data are enciphered was shown, it is also possible to use public key cryptosystems, such as RSA, for this part.

[0101] Moreover, the simplest example of a configuration of contents is shown in drawing 7 . In this example, contents consist of only contents bodies and processing of encryption etc. is not performed for a contents body, either. However, it is in the situation of being only specific plug-in that service can be offered using these contents. By the verification routine in plug-in, only when processing same with having mentioned above is performed and it is judged as a result of the judgment in the verification section that it is just, plug-in uses these contents and offers service.

[0102] Below, several examples of a configuration of the processing in the verification section of the verification routine explained in the example 1 are described using drawing 8 - drawing 11 . Drawing 8 - drawing 11 mainly show the configuration about the verification section 59 in a verification routine. Although it was shown here as a configuration which has a comparator 591 and the expected-value storage section 592 in the verification section 59 in order to clarify the difference in each example of a configuration, not only this but the expected-value storage section 592 etc. may be constituted on the outside of the verification section 59.

[0103] (1) 1 of the example of a configuration of the verification section 59 is shown in drawing 8 . In this example of a configuration, the verification section 59 had the expected-value storage section 592 and a comparator 591, and has memorized the expected value A expected as certification data in the expected-value storage section 592. When the random-number effectiveness is given to the certification data received from the certification program to the input to the verification section 59, or an authentication data generate time, the certification data which removed the random-number effectiveness from the received certification data are inputted. A comparator 591 compares the expected value A remembered to be this inputted certification data A' in the expected-value storage section 592. When judged with it being just as a result of a comparison, delivery and a display display data for a just judgment on a display (decode / display 61).

[0104] In this configuration, the expected value A memorized in the expected-value storage section 592 is not unable to steal by a program analysis etc., even if difficult. If expected value A is stolen, it will become possible to constitute the equipment which copies [that the random number at the time of giving the random-number effectiveness can be expected, and] actuation of a certification program, and unlawful access by spoofing will be attained. In order to prevent such a thing, on the other hand, using tropism function h() as expected value whose conversion to hard flow has a difficult property and which is memorized in the expected-value storage section 592 To memorize data h (A) obtained by on the other hand giving tropism function h() to A, and what is necessary is just made to perform the comparison with the data h of the result of on the other hand having given tropism function h() (A') to certification data A' inputted into the verification section 591. Thus, since it is remarkably difficult to calculate h (A) to A even if expected-value h (A) memorized in the expected-value storage section 592 should be stolen with constituting, the above spoofing can be prevented.

[0105] (2) 2 of the example of a configuration of the verification section 59 is shown in drawing 9 . In this example of a configuration, the verification section 59 had the expected-value storage section 592, and a comparator 591 and the decode key storage section 593, and has memorized the expected value A expected as certification data in the expected-value storage section 592. When the random-number effectiveness is given to the certification data received from the certification program to the input to the verification section 59, or an authentication data generate time, the certification data which removed the random-number effectiveness from the received certification data are inputted. A comparator compares the expected value A remembered to be this inputted certification data A' in the expected-value storage section 592. When judged with it being just as a result of a comparison, delivery, and the decode/display 61 use this decode key K for decode / display 61 for the decode key K from the decode key storage section 593, encryption data are decoded, and data are displayed.
[0106] It is possible to use tropism function h() on the other hand as well as the example 1 of a configuration.
[0107] (3) 3 of the example of a configuration of the verification section 59 is shown in drawing 10 . In this example of a configuration, like the example 1 of a configuration, although the verification section 59 has the expected-value storage section 592 and a comparator 591, it has memorized the decode key K as expected value in the expected-value storage section 592. A comparator 591 compares the expected value K remembered to be inputted certification data K' in the expected-value storage section 592 like the example 1 of a configuration. When judged with it being just as a result of a comparison, delivery, and the decode/display 61 use this decode key K for decode / display 61 for decode key K', encryption data are decoded, and data are displayed.
[0108] (4) 4 of the example of a configuration of the verification section 59 is shown in drawing 11 . In this example of a configuration, the verification section 59 has the redundancy Banking Inspection Department 594. When the random-number effectiveness is given to the certification data received from the certification program to the input to the verification section 59, or an authentication data generate time, the certification data which removed the random-number effectiveness from the received certification data are inputted. This inputted certification data K' is inspected in the redundancy Banking Inspection Department 594. This approach gives redundancy beforehand to K, as mentioned above, and it inspects whether K' has that redundancy. For example, approaches, such as an international standard ISO 9796, can be used. If inspection of redundancy is passed in the redundancy Banking Inspection Department 594, the redundancy Banking Inspection Department 594 will use decode key K' for decode / display 61, delivery, and the decode/display 61 will use this decode key K, encryption data will be decoded, and data will be displayed.
[0109] [Example 2] The example 2 of this invention is explained below. That it is data with which the certification data generated by certification data generation equipment 11 were generated in the example 1 of this invention based on the data for verification, and the description information on access rating authentication It restricts to the time when the verification routine 15 of certification data verification equipment 10 verified, and the justification of certification data was verified. The example which unified the certification data verification routine 15 and the decode program 35, and was included in the Internet browser as a plug-in module about the service provision equipment with which service is offered was described. It was what the result of having removed the random-number effectiveness from the certification data which the verification routine 15 received in the example 1 becomes a decode key for decoding by decode/display, and judges whether the decode key is just, decodes encryption data using the decode key only when just, and offers service.
[0110] However, it is not necessary to necessarily judge the justification of the decode key like an example 1 in the example using the result of having removed the random-number effectiveness from certification data, as a decode key. It becomes possible for decode to be correctly successful and to offer service, in being a just decode key by decoding encryption data, using the result of having removed the random-number effectiveness from certification data, as a decode key as it is, and in not being a just decode key, decode only brings the result that service cannot be offered, without succeeding.
[0111] An example 2 explains the example which does not have the verification section in this way.

Hereafter, in the example 2, although the word verification "routine" is used, the verification section does not exist in this verification routine. That is, the part which judges whether verification was successful does not exist. An access ticket public key (E, n) and the authentication data KE are taken out from the enciphered contents, and the data for authentication are generated using them, it transmits to a certification program, and processing which passes the result of having removed the random-number effectiveness from the certification data returned from the certification program to decode/display, as a decode key is performed.

[0112] Drawing 12 shows the example of a configuration of an example 2. Drawing 12 is the configuration of having lost the verification section 59 from drawing 4 , and is the same configuration as drawing 4 except it.

[0113] Also about actuation, it is almost as the same as the example 1 explained, and [step 1] - [step 7] performs the same processing. Hereafter, [step 8] or subsequent ones is explained.

[0114] [Step 8]: End processing of a verification routine by step 7, and pass a verification routine to decode / display 61 by using as a decode key K' calculated in said random-number effectiveness removal section 58.

[0115] [Step 9]: Decode / display 61 decodes and displays the enciphered contents which separated decode key K' from the random-number effectiveness removal section 58 of a verification routine in reception and the data separation section 56. In a certification program, only when a user with a just token generates certification data using a just access ticket, decode key K' becomes a right decode key, and the enciphered contents are decoded correctly and it is displayed. When a token or an access ticket is not just, decode key K' cannot become a right decode key, and since the enciphered contents are not decoded correctly, it will not be indicated by the right.

[0116] [Example 3] The example 3 of this invention is explained below. Drawing 13 shows the configuration of the example 3 of this invention. The above is an example using a different protocol in a certification data verification side, and this example 3 is close to the configuration which advanced the component of the verification section shown by drawing 8 (b) of an example 1 out of the verification section. The same number has shown drawing 4 and a corresponding thing. In drawing 13 , 81 expresses the decode key storage section and the verification routine has held the decode key K for decoding contents beforehand.

[0117] The configuration of the enciphered contents consists of an enciphered contents body and an access ticket public key, and does not need to contain authentication data.

[0118] Next, actuation is explained. All the variables in the following explanation are integers.

[0119] [Step 1]: If a user demands use of the contents enciphered from the Internet browser, the Internet browser will look at the data type of the enciphered contents, and will load and start it in search of plug-in related with the data type. If corresponding plug-in starts, the verification routine 15 in plug-in will start. The contents in this case point out what a user uses through the Internet browser, for example, it is the display information on a homepage (an image, an animation, hyper-document, etc.), or they are programs like a Java applet.

[0120] [Step 2]: The verification routine 15 of plug-in takes out an access ticket public key (E, n) from the contents enciphered in the data separation section, and stores it in the access ticket public key storage section 51.

[0121] [Step 3]:, next the verification routine 15 generate a random number r in the random-number generation section 53, store it in the random-number storage section 54, and transmit Challenge C and the number n of access ticket public key methods (the number of the RSA methods) to a certification data generation side by setting a random number r to transmit data (challenge) C. in this case, the certification data which the program for certification returns -- Challenge C -- law -- it should become what is the basis of a number n and was enciphered using RSA cryptograph -- it comes out.

[0122] [Step 4]: In the program for certification, receive Challenge C and the number n of the RSA methods which were sent from the verification routine in the data receive section for authentication, and it is the following, and make and generate the certification data (response) R. First, in the 1st operation part, the access ticket t which uses the number n of the RSA methods as a key, and corresponds is

acquired, under the number n of the RSA methods, a formula 6 is performed and middle information R' is obtained from the access ticket storage section 72.
[0123] [step 5]: -- the user proper information e that the 2nd operation part 75 is memorized by the user proper information storage section 74 -- acquiring -- a formula 7 -- performing -- difference -- Information S is acquired.
[0124] [step 6]: and the certification data generation section 76 -- middle information [from the 1st and 2nd operation part 75] R', and difference -- Information S is acquired, a formula 8 is calculated and the certification data R are obtained. The certification data R are transmitted to a verification side.
[0125] [Step 7]: The verification section 59 of the verification routine 15 acquires the received certification data R, and verifies by comparing the random number r and count result r' which calculate a formula 10 and are memorized by the random-number storage section 54.
[0126]
[Equation 10] (10) The r'=RE mod n random number r and count result r' are regarded as verification having been successful, when equal, and the verification routine 15 passes the decode key K to decode/display.
[0127] [Step 8]: Decode / display 61 decodes and displays the enciphered contents which separated the decode key K from the verification section 59 in reception and the data separation section 56. It is more desirable for plug-in to display directly on the field which the Internet browser specified from the field of safety, since the decoded information may be copied by the Internet browser, although the approach of passing the decoded contents to the Internet browser and displaying by the Internet browser is also possible.
[0128] Thus, when it only verifies that a user has a just right and verification is successful, you may make it decode the contents enciphered with the decode key registered beforehand by the verification routine.
[0129] Although the example which constitutes the part of a verification routine from the above 1st thru/or an example 3 by the software program was shown, the decode key K of contents must be made secret in that case. Because, anyone can decode the contents enciphered as K will be revealed, and they will allow unjust use of contents. Therefore, a verification routine needs to protect an in-house data by a certain approach. As such an approach, in case a program is coded to a machine language, there is the approach of difficulty-in-reading-izing so that it may be hard to analyze an in-house data and a program procedure and they may become. These techniques are introduced by the Takanori Murakami "difficulty-in-reading-ized of program code" Institute of Electronics, Information and Communication Engineers technical research report (IEICE Technical Report) information security, ISEC 95-25 (1995), etc. Moreover, the approach of constituting a verification routine and a decode program from one hardware in addition to the software-based technique may be used. In that case, it can constitute from hardware, a PC card, an IC card of dedication, etc. Moreover, it is also possible to constitute all verification routines, certification data generation sections, and decode/displays from one hardware.
[0130] [Example 4] The example 4 of this invention is explained below. This example explains the example of a configuration which used use control information. Use control information is the control information for controlling generation of certification data, and is control information which describes the conditions which offer service, and is distributed with an access ticket. When not agreeing on conditions, as control information checks these conditions when the term which offers service, a tariff frame, a count, time amount, etc. can be described and certification data are generated, and it does not generate certification data, it can stop offer of service. To control information, the attribute of users, such as an executive, sex, and age, is described besides this, and it is also possible to control generation of certification data as compared with a user's attribute currently held in the token.
[0131] Below, the explanation when using a use term as control information and the explanation when using a tariff frame are described briefly.
[0132] In this example, the access ticket t is data generated based on the following formula 11.
[0133]
[Equation 11]

(11) t=D-F(n,e,L)
the 3 variable function with which, as for the 3 variable function F (x y, z), a function value cannot collide easily -- it is -- for example, the above-mentioned -- on the other hand, it can set like a formula 13 using tropism Hash Function h.
[0134]
[Equation 12]
(12) F(x,y,z)=h(x|y|z)
All the notations in an upper type are integers, like an example 1, the number of the RSA methods and D express an access ticket private key, and, as for e, n expresses user proper information. L is use control information and, on the other hand, function F() is a tropism function.
[0135] With reference to drawing 14 , this example is further explained to a detail. Drawing 14 shows concretely the example of a configuration of the example 4 of this invention. The left half of drawing 14 , i.e., plug-in, and verification routine side is the same as drawing 4 of an example 1.
[0136] The program 32 for certification consists of the data receive section 71 for authentication, the access ticket storage section 72, the 1st operation part 73, and the certification data generation section 76, and a token 33 consists of the user proper information storage section 74, the 2nd operation part 75, and the use control information judging section 77.
[0137] In addition to the number n of the RSA methods, and the access ticket t, the access ticket storage section 72 made use control information L the group, and has memorized it. The use control information judging section 77 passes the use control information L to the 2nd operation part 75, only when the conditions of the use control information L passed from the access ticket storage section 72 are judged and it judges with the right as a result of a judgment. the time of the use control information L being passed from the use control information judging section 77 in the 2nd operation part 75 -- a formula 13 -- being based -- difference -- Information S is calculated and it sends to the certification data generation section 76.
[0138]
[Equation 13]
(13) S=CF (n, e, L) mod The time of using a use term as use control information is explained below by n. When it has a use term as use control information, the value of the use control information L is a value like 199712312400. In this case, this value expresses that a use term is 24:00 on December 31, 1997. It does not matter as for expressing with the relative number of seconds from a certain time instead of such a figure etc.
[0139] The use control information judging section 77 in a token has a clock, and compares with current time of day the use control information L passed from the access ticket storage section 72. And when the value of the use control information L is the back [time of day / current] as a result of a comparison, it judges with the right and the use control information L is passed to the 2nd operation part 75. the time of the use control information L being passed from the use control information judging section 77 in the 2nd operation part 75 -- a formula 13 -- being based -- difference -- Information S is calculated and it sends to the certification data generation section 76.
[0140] Henceforth, like an example 1, the certification data R are calculated using a formula 8 in the certification data generation section 76, in the random-number effectiveness removal section 58 of the verification routine 15, the certification data R received in the certification data receive section 57 are acquired, a formula 9 is calculated with the random number r memorized by the random-number storage section 54, and K' is obtained.
[0141] Whenever count was made using the right access ticket t, the right user proper information e, and the right use control information L, K'=K is realized, the judgment with the right is made by the verification section of the verification routine 15, and service is offered. It is going to use the access ticket with which the use term of the use control information L has expired, and since the access ticket t cannot be altered even if it alters the use control information L it is remembered to be by the access ticket storage section 72 whether you are whom, it cannot become in a right value and the certification data R generated using the formula 8 in the certification data generation section 76 cannot receive offer

of service unfairly.
[0142] When the use control information L is the amount of use of service, the figure 100 is given once in 100 yen semantics as a value of for example, the use control information L.
[0143] A token has the prepaid balance storage section which memorizes prepaid balance information, and the use control information judging section 77 in a token compares the use control information L with the prepaid balance, when the prepaid balance is larger, it judges with the right, reduces the value which corresponds in use control information L minutes from the prepaid balance, and passes the use control information L to the 2nd operation part 75. The following processings are the same.
[0144] Moreover, it has the use hysteresis storage section, and the use control information judging section 77 in a token records the value of the use control information L on the use hysteresis storage section with information, such as time of day, and you may make it pass the use control information L to the 2nd operation part 75 instead of the prepaid balance storage section. In this case, it processes collecting the use hysteresis sometimes memorized by the use hysteresis storage section, and paying the corresponding amount of money etc.
[0145] Thus, also except the example shown here, after checking the use control information L by the use control information judging section 77, it becomes possible to perform various use control with constituting so that the use control information L may be passed to the 2nd operation part 75.
[0146] [Example 5] The example 5 of this invention is explained below. An example 5 is an example which distributes the contents encapsulated using satellite broadcasting service, and offers service. Here, it points out preventing from using, if contents are remained as it is by giving encryption etc. as capsulation. The schematic diagram of the service provision system which used satellite broadcasting service for drawing 15 is shown. The encapsulated contents are distributed to each user using satellite broadcasting service. A user receives a satellite electric wave with a satellite antenna, and inputs into a receiver 100. In a receiver, the service provision equipment of this invention is mounted, and when verification is successful, contents can be used.
[0147] The contents offered here can consider various things, such as a movie, music, a TV program, software, a photograph, reference, and news. Each contents are used in the television video 200 connected to the receiver 100, audio equipment 300, and (Computer PC) 400 grade. Here, although the example into which the receiver 100 and the service use device are divided is explained, the service use device by which the receiver 100 was built in can explain similarly.
[0148] The structure of the encapsulated contents is shown in drawing 16 . The encapsulated contents are classified into the data enciphered as the contents header. The contents header has the label, the public key (E, n), and the enciphered decode key for identifying contents. The enciphered data are equivalent to the contents body enciphered in the aforementioned example.
[0149] Drawing 17 is the example which showed the configuration of the receiver 100 in drawing 15 concretely. Each circuit of a receiver 100 is controlled by the microcomputer. The satellite signal from a satellite antenna is first inputted into the tuner 101 of a receiver 100. A tuner 101 extracts the data of the channel which the user chose with the panel of a receiver 100, or remote control. An error correction circuit / descrambling circuit 102 reverts as contents, and inputs the extracted data into the data control circuit 103. In the data control circuit 103, when it identifies with a contents label whether contents are encapsulated or not and contents are not encapsulated in it, an output side is passed as it is. Contents are inputted into verification / decoder circuit 104 when contents are encapsulated. Although it is possible in verification / decoder circuit 104 to verify justification by the verification routine shown in the old example, an example 5 shows and explains an option. The detail of this approach is explained with reference to drawing 18 . In addition, the decoded data are supplied to a use device as a signal which the video decoder 106 or the audio decoder 107 is sent through a demultiplexing circuit 105, and corresponds.
[0150] The verification procedure (protocol) of an example 5 is shown in drawing 18 . The same number has shown the part which has the same function as an example 1.
[0151] The access ticket t in an example 5 is data generated based on a formula 14.
[0152]

[Equation 14] (14) t=D-F(n,e)
All the notations in an upper type are integers, and express the following. (Refer to the formula of an example 1)
n is the product of the number p and q of the RSA methods, i.e., the two sufficiently big prime factors, (n=pq). phi (n) is the Euler number of n, i.e., the product of p-1 and q-1, (phi (n) = (p-1) (q-1)). e expresses user proper information, it is a different number for every user, and it uses it in order to identify a user. D -- an access ticket private key -- expressing -- law -- it is a RSA private key under a number n, and a formula 2 is filled. Here, gcd (x y) expresses the greatest common measure of more than 2 [x] and y.
[0153] The property expressed by the formula (2) guarantees that several E which fills a formula 3 exists. E is called an access ticket public key.
[0154] the 2 variable function with which, as for the 2 variable function F (x y), a function value cannot collide easily -- it is -- for example, the above-mentioned -- on the other hand, it can set like a formula 15 using tropism Hash Function h.
[0155]
[Equation 15]
(15) F(x,y)=h(x|y)
An example 5 is explained to a detail using a Fig. below. The verification / decoder circuit 104 in drawing 17 are shown by 38 at drawing 18 . Verification / decoder circuit 38 consists of a verification routine 15 and the decode section 61, it is realizing by ASIC (application specificintegrated circuit) etc. and the safety of high-speed processing of decode or a verification routine is guaranteed. It is also possible to, realize verification / decoder circuit 38 by the software program, of course. Moreover, in order to raise safety more, you may constitute from hardware which has the Tampa-proof property mentioned above. In verification/decoder circuit, the encapsulated contents which were received from the data control circuit are divided into the data enciphered as the contents header in the data separation section 56, and the data enciphered by the authentication data storage section 52 in the decode key KE enciphered by the access ticket public key storage section 51 in the public key (E, n) are stored in the decode section 61, respectively. And while verification/decoder circuit generates a random number in the internal random-number generation section and memorizes it in the random-number storage section 54, it calculates transmit data C based on a formula 5 in the transmit data count section like an example 1.
[0156] thus, calculated transmit data C -- law -- it is transmitted to a certification program together with a number n.
[0157] The operation of the 1st operation part 73 of a certification program and the certification data generation section 76 is performed with a microcomputer, and the access ticket is memorized by EPROM (erasableprogrammable read only memory) etc. Authentication data choose the access ticket [/ based on n which received] t, it is the basis of the number n of the RSA methods received from the authentication data receive section 71, and perform a formula 16 and obtain middle information R' from the access ticket storage section 72.
[0158]
[Equation 16]
(16) R'=Ct mod an IC card realizes n token -- having -- the user proper information storage section 74 and the 2nd operation part 75 -- having -- a microcomputer to the data for authentication -- receiving -- a formula 17 -- performing -- difference -- Information S is acquired.
[0159]
[Equation 17]
(17) S=CF (n, e) mod n and the certification data generation section 75 of a certification program -- middle information [from the 1st and 2nd operation part 73 and 75] R', and difference -- Information S is acquired, a formula 18 is calculated and the certification data R are obtained.
[0160]
[Equation 18] (18) R=R'S mod n, thus the obtained certification data R are transmitted to the

certification data receive section 57 of verification/decoder circuit.
[0161] The random-number effectiveness removal section 58 of the verification routine 15 acquires the certification data R received in the data receive section 57, calculates a formula 19 with the random number r memorized by the random-number storage section 54, and obtains the decode key K.
[0162]
[Equation 19] (19) K=Rr -1 mod n -- redundancy is given to K at this time and you may make it verify whether the decode key K was correctly decoded by giving a specific value to that part in the verification section 59 The obtained decode key K is inputted into the decode section 61, in the decode section 61, decodes the enciphered data using the decode key K, and outputs them as contents.
[0163] The outputted contents are used with PC as digital data, or are used as image information or audio information.
[0164] The general-view Fig. of the service provision equipment of this example is shown in drawing 19 . As shown in drawing, service provision equipment is connected to television. Although not shown in drawing, while it connects with the satellite antenna and service provision equipment receives satellite broadcasting service, it connects with the network through the modem and it can acquire the access ticket for using the encapsulated contents which received by satellite broadcasting service. As shown in drawing 19 (a), when contents are enciphered and the token is not being inserted in service provision equipment, a user cannot see an image. Then, if a user acquires a just access ticket and a token is inserted in service provision equipment, as shown in drawing 19 (b), he can see an image.
[0165] Thus, in this invention, in spite of enciphering and offering contents by one cryptographic key, if it does not have both of tokens which stored the access ticket customized for every user, and user proper information, service can be used no longer. Therefore, contents are enciphered, and the provider (provider) of contents can be provided using the mass media like satellite broadcasting service, and can perform positive use management for every user by the access ticket and the token.
[0166] [Example 6] The example 6 of this invention is explained below. Although the above described the case where it encapsulated for every contents, the encryption same about the broadcast channel of satellite broadcasting service is given as applications other than this, and there is a case where he wants to restrict use of contents by managing viewing-and-listening time amount etc. Such service is realized by expressing an access ticket by the formula 20.
[0167]
[Equation 20] (20) t=D-F(n,e,L)
Here, L is use control information and expresses a use term. the 3 variable function with which, as for the 3 variable function F (x y, z), a function value cannot collide easily -- it is -- for example, the above-mentioned -- on the other hand, it can set like a formula 21 using tropism Hash Function h.
[0168]
[Equation 21]
(21) F(x,y,z)=h(x|y|z)
The example of a configuration of use control information is shown in drawing 20. The use control information L consists of use start time, use end time, and a use tariff as shown in drawing. A use tariff is required only when a token has a prepaid function, and when not using a prepaid function, it can be omitted. The verification protocol at the time of using the use control information L for drawing 21 is shown. The same number has shown the thing of the same function as drawing 18 here.
[0169] Hereafter, an example 6 is explained to a detail using drawing. In verification/decoder circuit, the encapsulated contents which were received from the data control circuit are divided into the data enciphered as the contents header in the data separation section 56, and the data enciphered by the authentication data storage section 52 in the decode key KE enciphered by the access ticket public key storage section 51 in the public key (E, n) are stored in the decode section 61, respectively. And while verification/decoder circuit generates a random number in the internal random-number generation section and memorizes it in the random-number storage section 54, it calculates transmit data C based on a formula 15 in the transmit data count section.
[0170] thus, calculated transmit data C -- law -- it is transmitted to a certification program together with

a number n.
[0171] The operation of the 1st operation part 73 of a certification program and the certification data generation section 76 is performed with a microcomputer, and the access ticket is memorized by EPROM (erasableprogrammable read only memory) etc. Authentication data choose the access ticket t and the use control information L, it is the basis of the number n of the RSA methods received from the authentication data receive section 71, and perform a formula 16 and obtain middle information R' from the access ticket storage section 72. [/ based on n which received]
[0172] A token has the user proper information storage section 74 and the 2nd operation part 75, and has prepaid frequency and token time-of-day data further. A token verifies whether the expiration date in reception and use control information is contradictory to token time of day in the data for authentication, and the use control information L from a microcomputer. That is, when use start time <= token time-of-day <= use end time has come, it is considered that verification was successful. If it succeeds in verification of an expiration date, it checks that the frequency of a token remains more than the number of availabilities within the use control information L, and if it remains, several availability minutes in the use control information L will be subtracted from the frequency of a token. When verification of an expiration date went wrong, and when frequency is insufficient, it does not process but an error is returned. the case where the above-mentioned verification is successful -- a formula 22 -- performing -- difference -- Information S is acquired.
[0173]
[Equation 22]
(22) S=CF (n, e, L) mod n and the certification data generation section 75 of a certification program -- middle information [from the 1st and 2nd operation part 73 and 75] R', and difference -- Information S is acquired, a formula 18 is calculated and the certification data R are obtained. Thus, the obtained certification data R are transmitted to the certification data receive section 57 of verification/decoder circuit.
[0174] The random-number effectiveness removal section 58 of the verification routine 15 acquires the certification data R received in the data receive section 57, calculates a formula 19 with the random number r memorized by the random-number storage section 54, and obtains the decode key K. Here, when the use control information L used by the token is altered, an exact decode key cannot be taken out. Redundancy is given to K at this time and you may make it verify whether the decode key K was correctly decoded by giving a specific value to that part in the verification section 59. The obtained decode key K is inputted into the decode section 61, in the decode section 61, decodes the enciphered data using the decode key K, and outputs them as contents.
[0175] The outputted contents are used with PC as digital data, or are used as image information or audio information.
[0176] In this example, although time of day is given to the token, since there is no clock in the interior when using an IC card, it is necessary to guarantee the justification of token time of day.
[0177] It is also possible to be able to set up the right of use for every time amount, and to realize functions, such as pay-per-view, by doing in this way, though he cannot use an access ticket unless a user is within the expiration date in use control information, but the contents of one channel are enciphered by the same cryptographic key.
[0178] In addition, this invention is not limited to an above-mentioned example, and use of contents can be performed through various record media, communication media, and a broadcast medium. It can apply, when using the various communication media and the broadcast medium other than the Internet and satellite broadcasting service. For example, it is applicable also to offer of service of the online karaoke by the usual telephone network, the data communication network, and TCP/IP connection.
[0179]
[Effect of the Invention] It will end, if the description information and user proper information on access rating authentication can be made to become independent, therefore the protection side and user side also prepares one proper information by introducing the auxiliary data for certification (access ticket) according to this invention, as explained above. An access ticket is data calculated based on specific user

proper information and the description information on access rating authentication, and it is impossible to ******** to calculate the description information on access rating authentication for user proper information from an access ticket to not knowing at least. And since service is offered only when user proper information and an access ticket are right and it is put together (contents are decoded), a user can possess user proper information beforehand and the user proper information that a user possesses a service provider can prepare the description information on access rating authentication independently. Even when it follows, for example, contents are enciphered by one cryptographic key, the need of becoming possible to assign an access privilege only to a desired user, and preparing the enciphered contents for every user is lost.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL FIELD

[Field of the Invention] This invention relates to the service provision equipment which can provide with service alternatively only the user who has a just right, and its approach.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

EFFECT OF THE INVENTION

[Effect of the Invention] It will end, if the description information and user proper information on access rating authentication can be made to become independent, therefore the protection side and user side also prepares one proper information by introducing the auxiliary data for certification (access ticket) according to this invention, as explained above. An access ticket is data calculated based on specific user proper information and the description information on access rating authentication, and it is impossible to ******** to calculate the description information on access rating authentication for user proper information from an access ticket to not knowing at least. And since service is offered only when user proper information and an access ticket are right and it is put together (contents are decoded), a user can possess user proper information beforehand and the user proper information that a user possesses a service provider can prepare the description information on access rating authentication independently. Even when it follows, for example, contents are enciphered by one cryptographic key, the need of becoming possible to assign an access privilege only to a desired user, and preparing the enciphered contents for every user is lost.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

PRIOR ART

[Description of the Prior Art] The time which various information is digitized by development of a network in recent years, and circulates through a network by it has come. As information digitized, there are an end still picture, an animation, voice, a program, etc. about text, and we can receive various services which combined these on the network. However, the ease of the copy which is the big description of these digital information had become the factor which checks circulation of the digital information in a network until now. Since this can generate the completely same object as original if digital information is copied, what once circulated is used without notice in the place which an author does not mean, and it originates in the problem of being hard to collect the just countervalues which an author should get.
[0003] In order to solve this problem, recently, encipher digital information and it is made to circulate freely like CD-SHOWCASE (a trademark or product name) of IBM Japan Corp., and in case it uses, price is paid and a system which uses reception and digital information for a decode key by the telephone line etc. has also appeared. Moreover, the example of the system which charges according to the amount using software and collects tariffs is shown in the "software management method" of JP,6-95302,B. The amount measuring device of information use which can measure exactly the amounts of use, such as information utilization time of all the users of the information distributed by broadcast, is described by the "amount measuring device of information use" of JP,7-21276,B. According to this, the amount measuring device of information use receives and accumulates the enciphered books information, and the example for which the user records the time amount and the amount which decoded and displayed books information as use hysteresis, and collects a tariff by that cause is shown.
[0004] Various code techniques as an approach and the program execution control technique of realizing the aforementioned system are known as advanced technology.
[0005] The user who has tried activation of application inspects holding the key for authentication of normal, ** this routine is restricted when existence of the key for the ** aforementioned authentication is checked, a program execution control technique embeds the routine for a user's access rating authentication into ** application program, and it continues a program, and when other, it is the technique which stops program execution. By using this technique, if only the user of the normal which holds an authentication key is possible, he can close activation of application. It is put in practical use in the software **** enterprise and this technique is RainbowTechnologies as a product, for example. Sentinel of an Inc. company SuperPro (trademark) and Aladdin Knowledge Systems There is an HASP (trademark) of a Ltd. company etc.
[0006] A program execution control technique is explained more below at a detail.
** The user who performs software holds an authentication key as user proper information. An authentication key is a key for encryption and those who permit use of software, for example, a software vendor, distribute it to a user. An authentication key is severely enclosed with the memory in hardware, in order to prevent a duplicate, and it is delivered by the user using a postal physical means.
** Equip an owner's personal computer or workstation by the approach which had the hardware which built in the user authentication key specified. A printer port etc. is equipped with hardware.

** If a user starts an application program and program execution attains to said access rating authentication routine, a program will communicate with the hardware which built in a user's authentication key. If a program identifies an authentication key and existence of a right authentication key is checked based on a communication link result, activation will be moved to the following step. When a communication link goes wrong and existence of an authentication key is not checked, a program stops oneself and can be made not to perform subsequent activation.
[0007] Discernment of the authentication key by the access rating authentication routine is performed by the following protocols, for example.
** An access rating authentication routine generates a suitable number, and transmits to hardware with a built-in key.
** The hardware with a built-in key enciphers the number sent using the authentication key to build in, and answers said access rating authentication routine.
** An authentication routine judges whether it is the number with which the answered number enciphers the number expected beforehand, i.e., the number transmitted to hardware, with a right authentication key, and is obtained.
** It continues program execution, in being in agreement with the number with which the number with which a letter was answered was expected, and in not being in agreement, it stops a program.
[0008] Even if the application program in this case and the communication link between hardware with a built-in authentication key are exchanged between the same hardware in the same part in the same application program, they must differ at every activation. Otherwise, it will also enable the user who does not hold a right authentication key to perform a program by answering an application program in the contents of a communication link which recorded the contents of a communication link in a normal activation process once, and were recorded whenever it performed the program after that. Such an attack is called a replay attack.
[0009] In order to prevent a replay attack, the number usually sent to hardware with a built-in key uses the random number newly generated at every communication link.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL PROBLEM

The trouble of the [trouble of conventional technique] conventional technique originates in the property in which protection processing of a program must be performed based on this authentication key, after a programmer assumes beforehand the authentication key which a user has, when creating an application program.
[0011] That is, only when the right reply from hardware with a built-in key is beforehand carried out a side at the time of a programming and a right reply is received, the implementer of a program has to create a program so that a program may be performed normally.
[0012] Although the use gestalt of the conventional technique of having the aforementioned description becomes the two aforementioned kinds fundamentally, it has the problem which states below in any case.
[0013] ** By the 1st approach, prepare a user's authentication key so that it may differ for every user. That is, every one different authentication key for every user is prepared for the user first like authentication **** at authentication **** and the user second. In this case, the authentication routine in a program must be created so that the authentication key of the proper of the user using this program can be attested, and a programmer needs to create the program from which only the number of use users differs.
[0014] When the target users are a large number, the activity which customizes a program for every user (individualization) requires an effort intolerable for a programmer, and becomes what also has a huge list of user authentication keys which must be managed.
[0015] ** By the 2nd approach, the implementer of a program prepares an authentication key which is different for every application, respectively. That is, every one authentication key which is different for every application like authentication **** is prepared for the application first at authentication **** and the application second, and each application program is created so that the authentication key of a proper may be identified.
[0016] Although it becomes unnecessary to create a program individually for every user like the 1st approach by this approach, as for a user, only the number of the applications to be used must hold an authentication key conversely.
[0017] As mentioned above, it is necessary to distribute an authentication key to a user in the condition of having enclosed with hardware severely. Therefore, it cannot but depend for distribution of the hardware which builds in an authentication key on a postal physical means to the ability to distribute the program itself simple through a network. the hardware with which the authentication key corresponding to [to whenever / upper ****** / in a programmer] the application for since [use consent / of the application from a user] was enclosed -- it is necessary to mail -- cost, time amount, and the time and effort of packing -- it becomes a very big burden for a programmer about any.
[0018] Moreover, a user must be content with the complicatedness that hardware must be exchanged whenever it changes the application to be used.
[0019] Though he wants to use application with a user, it must wait until the hardware with which the authentication key was enclosed is mailed and it arrives, and there is also a problem that it cannot use

immediately.
[0020] Although the approach of teaching a user the password for making the authentication key in hardware available whenever it encloses two or more authentication keys beforehand into hardware and permits a user use of new application can be used in order to mitigate these problems, when the authentication key enclosed beforehand is exhausted, the same problem occurs, and it has not become essential solution.
[0021] You may consider that it is hardly defended since a user can copy application so that he may like, once it decodes application by this approach, although the simple method of only enciphering application in addition to the approach of the above effective control, and teaching a user that decode key by the safe approach is used generally and widely, and it can distribute unjustly.
[0022] Therefore, when the digitized information, for example, software, music, a movie, etc. tended to be delivered in a network (these are henceforth called contents generically) and it was going to obtain a just countervalue, in a Prior art, there was a problem of management of contents becoming complicated or applying a big burden to a user by management of the hardware for authentication.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

MEANS

[Means for Solving the Problem] The 1st storage means which memorizes the data for authentication to the service provision equipment which provides with service only the user who has a just right in order to attain the above-mentioned purpose according to the 1st side face of this invention, The 2nd storage means which memorizes a user's proper information, and said user's proper information, The 3rd storage means which memorizes the auxiliary information for certification which it is as a result of activation that predetermined count was performed, to the description information on access rating authentication, The data for authentication currently held at said 1st storage means, and said user's proper information memorized by said 2nd storage means, He is trying to establish a certification data generation means to perform predetermined count to said auxiliary information for certification memorized by said 3rd storage means, and to generate certification data.
[0025] Moreover, the 1st storage means which memorizes the data for authentication to the service provision equipment which provides with service only the user who has a just right according to the 2nd side face of this invention, The 2nd storage means which memorizes a user's proper information, and said user's proper information, The 3rd storage means which memorizes the auxiliary information for certification which it is as a result of activation that predetermined count was performed, to the description information on access rating authentication, The data for authentication currently held at said 1st storage means, and said user's proper information memorized by said 2nd storage means, A certification data generation means to perform predetermined count to said auxiliary information for certification memorized by said 3rd storage means, and to generate certification data, He is trying to establish a certification data verification means to verify that the certification data generated by said certification data generation means are generated based on the description information on said access rating authentication.
[0026] According to these configurations, by introducing the auxiliary data for certification (access ticket) The description information for access rating authentication which is a protection side and is given, and the user proper information given to a user side can be made to become independent. A user possesses user proper information beforehand and protection persons, such as a programmer, create an application program using the description information on access rating authentication independently of the user proper information which a user possesses. Then, by creating and distributing an access ticket according to a user's **** information and the description information on the access ticket rating authentication used for creation of an application program etc. It becomes possible to attest user access ratings, such as execution control, and only the user who has a just right can be provided with desired service. Moreover, if a log is taken to a certification data generate time, the just countervalue to service is recoverable.
[0027] Moreover, you may make it held in the aforementioned configuration in a defense means to close if it is difficult for said 2nd storage means and said certification data generation means to observe an in-house data and processing procedure from the outside at least.
[0028] Moreover, you may make it held in the aforementioned configuration in a defense means to close if it is difficult for said certification data verification means to observe an in-house data and processing

procedure from the outside at least.
[0029] Moreover, the description information on said access rating authentication is a decode key in an encryption function, and data with said suitable data for authentication are enciphered using the encryption key corresponding to said decode key, and you may make it verify that the certification data which said certification data generation means generates decode said data for authentication correctly with said certification data verification means. Moreover, the description information on said access rating authentication is an encryption key in an encryption function, and said data for authentication decode suitable data using the decode key corresponding to said encryption key, and you may make it verify that the certification data which said certification data generation means generates encipher said data for authentication correctly with said certification data verification means. Moreover, you may make it verify that the certification data which the description information on said access rating authentication is a signature key in a digital signature function, and said certification data generation means generates are the digital signature correctly generated to said data for authentication using said signature key.
[0030] Moreover, the description information on said access rating authentication is the 1st decode key in an encryption function. Said data for authentication encipher the 2nd decode key which decodes said enciphered information using the encryption key corresponding to said 1st decode key. The certification data generated by said certification data generation means are said 2nd decode key, and said enciphered information is decoded using said 2nd decode key, and you may make it offer the service corresponding to said information. Moreover, said encryption function may be an unsymmetrical key encryption function, and the description information on access rating authentication may be one side of a key.
[0031] Moreover, said encryption function may be a public-key-encryption-ized function and the description information on access rating authentication may be a private key.
[0032] Moreover, said encryption function may be a symmetry key encryption function, and the description information on access rating authentication may be a common private key.
[0033] Moreover, said 1st storage means, said 2nd storage means, and said 3rd storage means, The certification data generation equipment which consists of said certification data generation means, and the 4th storage means which memorizes the data for authentication in addition to said certification data verification means, In the service provision equipment which has access rating authentication equipment with which the certification data verification equipment which offered the 5th storage means which memorizes certification data attests a user's access rating by communicating mutually Certification data verification equipment writes out the data for authentication memorized by the 4th storage means to the 1st storage means of certification data generation equipment. Certification data generation equipment The certification data generated based on said data for authentication written in the 1st storage means by the certification data generation means It rakes out for the 5th storage means in certification data verification equipment, and certification data verification equipment can attest a user's access rating using said certification data written in the 5th storage means.
[0034] The description information for access rating authentication is the decode key of an encryption function. Certification data verification equipment Moreover, a random-number generation means, While it has the 6th storage means which memorizes the generated random number, and the 7th storage means which memorizes the ** data for authentication and a random-number generation means writes the generated random number in the 6th storage means After giving the random-number effectiveness which used said random number for the ** data for authentication memorized by the 7th storage means, it writes in the 4th storage means as data for authentication. A certification data verification means The result of having removed the random-number effectiveness by the random number memorized by the 6th storage means from the certification data in which it was written by the 5th storage means with said certification data generation equipment You may make it verify decoding the ** data for authentication memorized by the 7th storage means with the decode key which is the description information on access rating authentication.
[0035] Moreover, the description information for access rating authentication is the encryption key of an encryption function, and certification data-verification equipment is equipped with a random-number

generation means, a random-number generation means writes in the 4th storage means by using the generated random number as the data for authentication, and it may make it verify that the certification data written in the 5th storage means by certification data generation equipment decode said random number in a certification data-verification means.
[0036] Moreover, the description information for access rating authentication is the signature key of a digital signature function. Certification data verification equipment is equipped with a random-number generation means, and a random-number generation means is written in the 4th storage means by using the generated random number as the data for authentication. A certification data verification means You may make it verify that the certification data written in the 5th storage means by certification data generation equipment are a digital signature with the signature key it is [key] the description information on access rating authentication to the data for authentication which are said random number.

[0037]
[The mode of implementation of invention] Hereafter, this invention is explained to a detail.
[Example 1] With reference to an example 1, the theoretic configuration of this invention is explained first. Drawing 1 shows the configuration of the example 1 of this invention as a whole, the service provision system consists of certification data verification equipment 10 and certification data generation equipment 11 in this drawing 1 , and certification data generation equipment 11 receives the access ticket (auxiliary data for certification) 13 from access ticket generation equipment 12. Certification data verification equipment 10 performs the verification routine 15. Certification data generation equipment 11 holds the user proper information 16 and the access ticket 13, and performs the certification data generator 17. A part of user proper information 16 and certification data generator [at least] 17 are protected with tamper-proof equipment 20.
[0038] Access ticket generation equipment 12 generates the access ticket 13 based on the description information 14 on access rating authentication, and a user's proper information 16, and the access ticket 13 is sent to a user through a network, a storage, etc., and is held at a user's certification data generation equipment 11.
[0039] Certification data verification equipment 10 transmits the data 18 for authentication to certification data generation equipment 11. Certification data generation equipment 11 generates the certification data 19 using the access ticket 13 and the user proper information 16, and answers certification data verification equipment 10 in this. Certification data verification equipment 10 verifies the justification of certification data based on the data for authentication. That is, it verifies that certification data are data generated based on the data for verification, and the description information on access rating authentication.
[0040] If the justification of certification data is verified, it will be attested that a user has a just right and desired service will be offered by service provision equipment.
[0041] Hereafter, taking the case of actual service, this invention is concretely explained using drawing 2 .
[0042] The example 1 of this invention describes the example which unified the certification data verification routine 15 and the decode program 35, and was included in the Internet browsers (trademark - of Netscape Navigator-U.S. Netscape Communications, Inc. etc.) as a plug-in (Plug-In) module. Here, a plug-in module can point out the software program which extends the function of the Internet browser, and, thereby, use of a new data type can be supported to a user. If the information on the data type which the Internet browser is not supporting is received from a server, the Internet browser will be loaded and started in search of plug-in related with the data type. Thereby, the support of a new data type is enabled seamlessly, without changing a user's existing system.
[0043] The contents 34 enciphered as the new data type in the case of this example are pointed out, and if the contents 34 as which the Internet browser was enciphered are received from a server, the Internet browser will look at the data type of the enciphered contents 34, and will be loaded and started in search of the plug-in 38 related with the data type. Started plug-in starts the verification routine 15, and verifies by using for the program 32 for certification delivery and the certification data to which it came on the

contrary for the data for authentication. When verification is successful with the verification routine 15, the enciphered contents 34 are decoded by the decode program 35, and it is provided for a user by it. The decoded contents are information, the downloaded programs, such as a hyper-document, an image, an animation, and music.

[0044] Certification data generation equipment consists of a program 32 for certification, and a token 33. The program 32 for authentication is a software program containing the access ticket 13 and the authentication data generator A36, and operates on a user's personal computer (PC). As for a token 33, it is desirable to constitute including the authentication data generator B37 and the user proper information 16 by the hardware (for it to be hereafter called the Tampa-proof hardware) which has the defense force to theft of the internal state by the probe. Because, user **** information is equivalent to the password in password authentication, and it is the important only information that a user's identity is proved, and when the user proper information 16 can be read, copied and distributed, a person without a just right will be allowed unjust use of contents.

[0045] Moreover, in addition to said user proper information, the certification data generators A and B which perform predetermined count procedure are given to a user. This program is for communicating with the verification routine 15 in plug-in 38, and if the user proper information 16 and the access ticket 13 are given, it will generate the certification data 45 which calculate to the data 42 for authentication and prove a user's identity. Although the user proper information 16 is used in process of this count, since there is a problem when the user proper information 16 is revealed outside for the reason mentioned above, the certification data generator B37 using user proper information is stored in said Tampa-proof hardware. IC chip protected by the IC card, resin mold, etc. is simple, and it is easy to apply it as Tampa-proof hardware. However, when the added value of the service to offer is very high, the equipment which has high safety as shown with "the encryption equipment, the decode equipment, the secret data processor, and information processor" of Japanese Patent Application No. No. 284475 [08 to] may be used.

[0046] Several operations of the certification data verification routine 15 are described below.

[0047] 1. Into the certification data verification routine 15, the reply data (expected value) it is expected that are data (data 42 for authentication) which should be transmitted are embedded. The certification data verification routine 15 takes out said transmit data, transmits to a user, and receives a reply from a user. Subsequently, when the reply data and said expected value from a user are compared and both are in agreement, the contents 34 enciphered by the decode program 35 are decoded, and a user is provided with contents in the available condition.

[0048] 2. Into the certification data verification routine 15, the reply data (expected value) it is expected that are data which should be transmitted are embedded. The certification data verification routine 15 takes out said transmit data, transmits to a user, and receives a reply from a user. Subsequently, the contents 34 enciphered by the decode program 35 in the value which gave the tropism function from the user to reply data on the other hand when both were in agreement as compared with said expected value are decoded, and a user is provided with contents in the available condition.

[0049] It sets to an operation of the above 1 and 2, and in being as a result of the encryption to which reply data follow the predetermined encryption algorithm of transmit data, the description information on access rating authentication serves as an encryption key. Moreover, in [reply data] being a digital signature according to the predetermined signature algorithm of transmit data, the description information on access rating authentication serves as a signature key.

[0050] 3. The data which should be transmitted are embedded into the certification data verification routine 15. The certification data verification routine 15 takes out said transmit data, transmits to a user, and receives a reply from a user. Subsequently, the contents 34 enciphered by the decode program 35 are decoded by using said reply data as a decode key, and a user is provided with contents in the available condition.

[0051] 4. The data which should be transmitted are embedded into the certification data verification routine 15. After the certification data verification routine 15 takes out said transmit data and gives the random-number effectiveness, it transmits to a user, and it receives a reply from a user. Subsequently,

the contents 34 enciphered by the decode program 35 are decoded by using as a decode key the result of having removed said random-number effectiveness from said reply data, and a user is provided with contents in the available condition.
[0052] 5. The certification data verification routine 15 receives the transmit data corresponding to the enciphered contents. In this case, the transmit data may be embedded in the enciphered contents. The certification data verification routine 15 transmits said received transmit data to a user, and receives a reply from a user. Subsequently, the contents 34 enciphered by the decode program 35 are decoded by using said reply data as a decode key, and a user is provided with contents in the available condition.
[0053] 6. The certification data verification routine 15 receives the transmit data corresponding to the enciphered contents. In this case, the transmit data may be embedded in the enciphered contents. The certification data verification routine 15 transmits to a user, after giving the random-number effectiveness to said received transmit data, and it receives a reply from a user. Subsequently, the contents 34 enciphered by the decode program 35 are decoded by using as a decode key the result of having removed said random-number effectiveness from said reply data, and a user is provided with contents in the available condition.
[0054] In the above 3 thru/or an operation of 6, when a right decode key is obtained from reply data, the contents 34 as which the hook was enciphered are decoded correctly, and a user becomes available about these contents. The description information on the access rating authentication in this case serves as a decode key for decoding the enciphered decode key.
[0055] Now, with the execution control technique stated in the conventional example, user proper information (a user's authentication key) is the same as the description information on access rating authentication. The conventional certification data generating routine calculates reply data by inputting the description information on access rating authentication, and the data transmitted from the certification data verification routine.
[0056] On the other hand, the user proper information 16 and the description information 14 on access rating authentication have the description of this invention in a mutually-independent point. In addition to the data 42 transmitted from the user proper information 16 and the certification data verification routine 15, the certification data generators A and B calculate the reply data (certification data) 45 also for this configuration by considering the access ticket 13 as an input. This configuration has the following properties.
[0057] 1. The access ticket 13 is data calculated based on the specific user proper information 16 and the description information 14 on access rating authentication.
2. It is impossible in computational complexity at least to calculate the description information 14 on access rating authentication for the user proper information 16 from the access ticket 13 to not knowing.
3. The certification data generators A and B calculate right reply data only within the case where the right combination of the user proper information 16 and the access ticket 13 is inputted, when the user proper information 16 and the access ticket 13 are right combination.
[0058] By the above, a user can possess the user proper information 16 beforehand, a contents implementer can encipher contents independently [the user proper information 16 which a user possesses], and the user proper information 16 can enjoy use of the contents enciphered independently only to the user who has a just right by creating the access ticket 13 according to the user proper information 16 and the description information on access rating authentication.
[0059] Moreover, the proper information which shall consist of two proper information and uses the user proper information 16 on the occasion of creation of the access ticket 13, and the proper information which a user uses in a communications program can also be distinguished and used. The most typical example is the approach of making user proper information 16 a public key pair, using for access ticket creation by making a public key into open proper information, and enclosing the private key in the token 33 as a user individual's secret proper information. In this case, by enabling it to calculate the access ticket 13 from the description information 14 on access rating authentication, and the public key of said public key pair, it becomes possible to calculate the access ticket 13, keeping secret the user proper information 16 which is a private key.

[0060] Next, a more concrete configuration is **(ed) and explained to an example. In drawing 2 , the Internet browser 31, plug-in 38, and the program 32 for certification are realizable as a software program on the computer 30 (PC or workstation) which a user uses. Although you may realize as a software program similarly about a token 33, in order to raise the safety of the proper information (user proper information) for identifying a user, it is desirable to use together the tokens 33 (an IC card, a PC card, board, etc.) which have the Tampa-proof property connected to this computer 30. Under the present circumstances, if the hardware which has portability like an IC card is used, it is convenient when a user works on two or more PCs or a workstation.
[0061] The enciphered contents 34 which are used by the Internet browser 31 are supplied to a user using storages, such as a network, CD-ROM, DVD, and a floppy disk.
[0062] If a user demands use of the contents enciphered from the Internet browser, the Internet browser will look at the data type of the enciphered contents, and will load and start it in search of plug-in related with the data type.
[0063] If plug-in starts, the verification program in this plug-in starts, it will communicate with the program 32 for certification, user authentication will be performed, and decode of these contents will be performed only within the case where a communication link is completed correctly.
[0064] In order to use the contents 34 as which the user was enciphered, it is necessary to acquire the access ticket (auxiliary information for certification) published by user him. A user equips said PC or workstation with an IC card, when user proper information is enclosed with the IC card, for example, while registering the acquired access ticket into the program 32 for certification installed on said PC or the workstation.
[0065] In harmony with certification data generator B, certification data generator A calculates based on the user proper information 16 and the access ticket 13, and performs the verification program 15 and communication link in plug-in based on the count.
[0066] As a result of a communication link, when [with the contents enciphered as user proper information and an access ticket] three correspond surely, it restricts that authentication by the verification program 15 is successful. Authentication is not successful when either user proper information or an access ticket is missing.
[0067] An access ticket is published by specific addressing to a user. That is, a specific user's user proper information is used on the occasion of generation of an access ticket. When the user proper information used for an access ticket generate time and said user proper information used by the certification data generator are not in agreement, authentication is not successful too.
[0068] Moreover, an access ticket is generated based on the description information on specific access rating authentication, and the verification program 15 is constituted so that the description information on this access rating authentication may be attested. Therefore, authentication is not successful also when the description information used as the basis of generation of an access ticket and the description information which the verification program 15 tends to attest do not correspond mutually.
[0069] Since it has safety sufficient in itself, an access ticket can be delivered through a network. The safeties of an access ticket are the following two properties.
[0070] 1. the user by whom an access ticket is a registered form and the access ticket was published -- only he (holder of the user proper information that it was correctly used for the access ticket generate time) can operate certification data generation equipment correctly using this access ticket. Therefore, even if a holder in bad faith intercepts a network and gets other users' access ticket unjustly, unless this third person gets the user proper information on the normal which is the issue place of an access ticket, it is impossible to use this access ticket.
[0071] 2. The access ticket holds still stricter safety. That is, even if a holder in bad faith collects the access tickets of the number of arbitration and performs what kind of analysis, it is impossible to constitute equipment which another access ticket is forged [equipment] based on the acquired information, or actuation of certification data generation equipment is copied [equipment], and forms authentication.
[0072] In the example 1, the access ticket t is data generated based on the following formula 1.

[0073]
[Equation 1]
(1) T=D-e+omegaphi (n)
All the notations in an upper type are integers, and express the following. n -- RSA (Rivest-Shamir-Adelman) -- law -- it is the product of a number p and q, i.e., the two sufficiently big prime factors, (n=pq). phi (n) is the Euler number of n, i.e., the product of p-1 and q-1, (phi (n) = (p-1) (q-1)). e expresses user proper information, it is a different number for every user, and it uses it in order to identify a user. D -- an access ticket private key, i.e., the description information on access rating authentication, -- expressing -- law -- it is a RSA private key under a number n, and a formula 2 is filled.

[0074]
[Equation 2] (2) gcd(D, phi (n)) =1 -- here, gcd (x y) expresses the greatest common measure of more than 2 [x] and y. The property expressed by the formula (2) guarantees that several E which fills a formula 3 exists.
[0075]
[Equation 3] (3) ED mod phi(n) =1E is called an access ticket public key.
[0076] omega is a number which becomes settled depending on n and e, and when n differs either from e, its value of the corresponds easily, twists it (it does not collide), and it is defined like. There is also a method of omega setting and on the other hand defining omega like a formula 4 as an example of the direction using tropism Hash Function h.
[0077]
[Equation 4] (4) Omega=h (n|e)
However, notation | expresses association of a bit string.
[0078] On the other hand, tropism Hash Functions are x which fills h(x) =h (y) and which is different from each other, and a function in which computing y has the property in which it is remarkable and difficult. On the other hand, it is RSA as an example of a tropism Hash Function. Data Security MD2 and MD4 by Inc., MD5, and the specification SHS (Secure Hash Standard) by the U.S. federal government are known.
[0079] In the number which appeared during the above-mentioned explanation, t, E, and n can be exhibited and D, e, omega, p, remaining q, and remaining phi (n) need to be secret in addition to those who have the right which creates a ticket.
[0080] The schematic diagram of the computer (PC or workstation) which a user uses for drawing 3 is shown. In drawing 3 , the card reader 39 is connected to the computer 30 which a user uses, and a user inserts and uses a token 33 for a card reader 39. The Internet browser 31, plug-in, and the program for certification are realized as a software program on a computer 30. Moreover, the access ticket is also memorized in the storage region of a computer 30. Now, the contents which it is going to use are the images of the picture of a yacht, and if a user with a just token and a just access ticket makes the enciphered contents read into the Internet browser 31, as shown in drawing 3 , the image of the picture of a yacht will be displayed on the Internet browser 31 by plug-in.
[0081] With reference to drawing 4 , an example 1 is further explained to a detail. Drawing 4 shows concretely the example of a configuration of the example 1 of this invention. If it is made to contrast with drawing 2 , the thing corresponding to the verification routine 15 consists of the access ticket public key storage section 51, the authentication data storage section 52, the random-number-generation section 53, the random-number storage section 54, the transmit data (challenge) count section 55, the data separation section 56, a certification data receive section 57, the random-number effectiveness removal section 58, and the verification section 59, and the decode program 35 runs on decode / display 61. Although a verification routine and a decode program are divided and being constituted from this example, a decode program may be made merged to a verification routine if needed. Moreover, the program 32 for certification consists of the data receive section 71 for authentication, the access ticket storage section 72, the 1st operation part 73, and the certification data generation section 76, and a token 33 consists of the user proper information storage section 74 and the 2nd operation part 75.

[0082] Next, actuation is explained. All the variables in the following explanation are integers.
[0083] [Step 1]: If a user demands use of the contents enciphered from the Internet browser, the Internet browser will look at the data type of the enciphered contents, and will load and start it in search of plug-in related with the data type. If corresponding plug-in starts, the verification routine 15 in plug-in will start. The contents in this case point out what a user uses through the Internet browser, for example, it is the display information on a homepage (an image, an animation, hyper-document, etc.), or they are programs like a Java applet.
[0084] [Step 2]: The verification routine 15 of plug-in takes out an access ticket public key (E, n) and the authentication data KE from the contents enciphered in the data separation section, and stores them in the access ticket public key storage section 51 and the authentication data storage section 52, respectively. Here, this access ticket public key and these authentication data were explained as what is distributed along with the enciphered contents. Thus, it is desirable to accompany the contents enciphered as this access ticket public key and these authentication data consider safety although they may accompany the enciphered contents and you may enable it to come to hand through a network, and, as for these authentication data, being embedded so that a user may not understand is still more desirable. For example, what is necessary is to encipher, to embed these authentication data into contents, and just to take the approach of decoding with the decode key given to plug-in, after taking out.
[0085] [Step 3]:, next the verification routine 15 generate a random number r in the random-number generation section 53, store it in the random-number storage section 54, and calculate transmit data (challenge) C according to a formula 5 using an access ticket public key (E, n), the authentication data KE, and a random number r.
[0086]
[Equation 5] (5) C=rEKE mod The n challenge C and the number n of access ticket public key methods (the number of the RSA methods) are transmitted to a certification data generation side. Since the random number r is contained in the value of C, it becomes a value which is different whenever it is a communication link, and has the effectiveness of preventing a replay attack.
[0087] [Step 4]: In the program for certification, receive Challenge C and the number n of the RSA methods which were sent from the verification routine in the data receive section for authentication, and it is the following, and make and generate the certification data (response) R. First, in the 1st operation part, the access ticket t which uses the number n of the RSA methods as a key, and corresponds is acquired, under the number n of the RSA methods, a formula 6 is performed and middle information R' is obtained from the access ticket storage section 72.
[0088]
[Equation 6] (6) R'=Ct mod n[step 5]: -- the user proper information e that the 2nd operation part 75 is memorized by the user proper information storage section 74 -- acquiring -- a formula 7 -- performing -- difference -- Information S is acquired.
[0089]
[Equation 7] (7) S=Ce mod n[step 6]: and the certification data generation section 76 -- middle information [from the 1st and 2nd operation part 73 and 75] R', and difference -- Information S is acquired, a formula 8 is calculated and the certification data R are obtained.
[0090]
[Equation 8] (8) R=R'S mod n certification data R are transmitted to a verification routine.
[0091] [Step 7]: The random-number effectiveness removal section 58 of the verification routine 15 acquires the certification data R received in the certification data receive section 57, calculates a formula 9 with the random number r memorized by the random-number storage section 54, and obtains K'.
[0092]
[Equation 9] (9) K -- verify that 'K calculated in said random-number effectiveness removal section 58 in the =Rr-1 mod n [step 8]:verification section 59' is generated based on D which is the description information on access rating authentication. K'=K should be realized when K' is generated based on D which is the description information on access rating authentication surely. Whether this formula is

realized has the approach of judging whether the data enciphered using this K' being decoded and it decoding correctly, the approach of judging by whether redundancy is given to K, the specific value is given to that part, and K' has that specific value, etc. Approaches, such as an international standard ISO 9796, can be used for the latter approach. Here, using the latter approach, explanation is continued on the assumption that it verifies.

[0093] [Step 9]: If verification in the verification section 59 is judged to be the right, a verification routine will pass decode key K' to decode / display 61.

[0094] [Step 10]: Decode / display 61 decodes and displays the enciphered contents which separated decode key K' from the verification section 59 in reception and the data separation section 56. It is more desirable for plug-in to display directly on the field which the Internet browser specified from the field of safety, since the decoded information may be copied by the Internet browser, although the approach of passing the decoded contents to the Internet browser and displaying by the Internet browser is also possible.

[0095] Thus, the user who has a just right can use the contents enciphered using the Internet browser. At this time, the decoded contents do not exist on temporary memory, but unjust use of the decoded contents can be prevented by making it disappear, after use of a user finishes.

[0096] By this example, the enciphered contents explained an access ticket public key (E, n) and the authentication data KE as what is accompanied and distributed. The example of a configuration of these enciphered contents is shown in drawing 5 . As shown in drawing 5 , the enciphered contents consist of contents bodies enciphered as an access ticket public key (E, n) and the authentication data KE. The data separation section of a verification routine reads these, and divides them into each part.

[0097] After the contents body is enciphered with Key K and verification is correctly completed using the authentication data KE, Key K can be restored through the random-number effectiveness removal section, and it becomes possible to decode a contents body using this key K.

[0098] In order to raise safety more, it is desirable to be embedded so that the authentication data KE cannot separate into a user easily. The one approach of this implementation is shown in drawing 6 . Although the enciphered contents consist of contents bodies enciphered as an access ticket public key (E, n) and the authentication data KE like drawing 5 at drawing 6 , not only a contents body but the authentication data KE are enciphered further. Drawing 6 showed the authentication data KE as what is enciphered with Key Kp.

[0099] The data separation section of a verification routine holds the decode key Kp corresponding to this cryptographic key key KP (the example using a common key encryptosystem), decodes the authentication data enciphered using the decode key KP which separated the contents body enciphered as the authentication data KE enciphered as the access ticket public key (E, n), and is held from the inputted whole contents, and takes out authentication data KE. Then, after verifying using this authentication data KE and completing verification correctly, Key K can be restored through the random-number effectiveness removal section, and it becomes possible to decode a contents body using this key K.

[0100] Although encryption and a decryption showed Key K and Key KP as an example using the same key since the example which used the common key encryption system here although a contents body and authentication data are enciphered was shown, it is also possible to use public key cryptosystems, such as RSA, for this part.

[0101] Moreover, the simplest example of a configuration of contents is shown in drawing 7 . In this example, contents consist of only contents bodies and processing of encryption etc. is not performed for a contents body, either. However, it is in the situation of being only specific plug-in that service can be offered using these contents. By the verification routine in plug-in, only when processing same with having mentioned above is performed and it is judged as a result of the judgment in the verification section that it is just, plug-in uses these contents and offers service.

[0102] Below, several examples of a configuration of the processing in the verification section of the verification routine explained in the example 1 are described using drawing 8 - drawing 11 . Drawing 8 - drawing 11 mainly show the configuration about the verification section 59 in a verification routine.

Although it was shown here as a configuration which has a comparator 591 and the expected-value storage section 592 in the verification section 59 in order to clarify the difference in each example of a configuration, not only this but the expected-value storage section 592 etc. may be constituted on the outside of the verification section 59.

[0103] (1) 1 of the example of a configuration of the verification section 59 is shown in drawing 8 . In this example of a configuration, the verification section 59 had the expected-value storage section 592 and a comparator 591, and has memorized the expected value A expected as certification data in the expected-value storage section 592. When the random-number effectiveness is given to the certification data received from the certification program to the input to the verification section 59, or an authentication data generate time, the certification data which removed the random-number effectiveness from the received certification data are inputted. A comparator 591 compares the expected value A remembered to be this inputted certification data A' in the expected-value storage section 592. When judged with it being just as a result of a comparison, delivery and a display display data for a just judgment on a display (decode / display 61).

[0104] In this configuration, the expected value A memorized in the expected-value storage section 592 is not unable to steal by a program analysis etc., even if difficult. If expected value A is stolen, it will become possible to constitute the equipment which copies [that the random number at the time of giving the random-number effectiveness can be expected, and] actuation of a certification program, and unlawful access by spoofing will be attained. In order to prevent such a thing, on the other hand, using tropism function h() as expected value whose conversion to hard flow has a difficult property and which is memorized in the expected-value storage section 592 To memorize data h (A) obtained by on the other hand giving tropism function h() to A, and what is necessary is just made to perform the comparison with the data h of the result of on the other hand having given tropism function h() (A') to certification data A' inputted into the verification section 591. Thus, since it is remarkably difficult to calculate h (A) to A even if expected-value h (A) memorized in the expected-value storage section 592 should be stolen with constituting, the above spoofing can be prevented.

[0105] (2) 2 of the example of a configuration of the verification section 59 is shown in drawing 9 . In this example of a configuration, the verification section 59 had the expected-value storage section 592, and a comparator 591 and the decode key storage section 593, and has memorized the expected value A expected as certification data in the expected-value storage section 592. When the random-number effectiveness is given to the certification data received from the certification program to the input to the verification section 59, or an authentication data generate time, the certification data which removed the random-number effectiveness from the received certification data are inputted. A comparator compares the expected value A remembered to be this inputted certification data A' in the expected-value storage section 592. When judged with it being just as a result of a comparison, delivery, and the decode/display 61 use this decode key K for decode / display 61 for the decode key K from the decode key storage section 593, encryption data are decoded, and data are displayed.

[0106] It is possible to use tropism function h() on the other hand as well as the example 1 of a configuration.

[0107] (3) 3 of the example of a configuration of the verification section 59 is shown in drawing 10 . In this example of a configuration, like the example 1 of a configuration, although the verification section 59 has the expected-value storage section 592 and a comparator 591, it has memorized the decode key K as expected value in the expected-value storage section 592. A comparator 591 compares the expected value K remembered to be inputted certification data K' in the expected-value storage section 592 like the example 1 of a configuration. When judged with it being just as a result of a comparison, delivery, and the decode/display 61 use this decode key K for decode / display 61 for decode key K', encryption data are decoded, and data are displayed.

[0108] (4) 4 of the example of a configuration of the verification section 59 is shown in drawing 11 . In this example of a configuration, the verification section 59 has the redundancy Banking Inspection Department 594. When the random-number effectiveness is given to the certification data received from the certification program to the input to the verification section 59, or an authentication data generate

time, the certification data which removed the random-number effectiveness from the received certification data are inputted. This inputted certification data K' is inspected in the redundancy Banking Inspection Department 594. This approach gives redundancy beforehand to K, as mentioned above, and it inspects whether K' has that redundancy. For example, approaches, such as an international standard ISO 9796, can be used. If inspection of redundancy is passed in the redundancy Banking Inspection Department 594, the redundancy Banking Inspection Department 594 will use decode key K' for decode / display 61, delivery, and the decode/display 61 will use this decode key K, encryption data will be decoded, and data will be displayed.

[0109] [Example 2] The example 2 of this invention is explained below. That it is data with which the certification data generated by certification data generation equipment 11 were generated in the example 1 of this invention based on the data for verification, and the description information on access rating authentication It restricts to the time when the verification routine 15 of certification data verification equipment 10 verified, and the justification of certification data was verified. The example which unified the certification data verification routine 15 and the decode program 35, and was included in the Internet browser as a plug-in module about the service provision equipment with which service is offered was described. It was what the result of having removed the random-number effectiveness from the certification data which the verification routine 15 received in the example 1 becomes a decode key for decoding by decode/display, and judges whether the decode key is just, decodes encryption data using the decode key only when just, and offers service.

[0110] However, it is not necessary to necessarily judge the justification of the decode key like an example 1 in the example using the result of having removed the random-number effectiveness from certification data, as a decode key. It becomes possible for decode to be correctly successful and to offer service, in being a just decode key by decoding encryption data, using the result of having removed the random-number effectiveness from certification data, as a decode key as it is, and in not being a just decode key, decode only brings the result that service cannot be offered, without succeeding.

[0111] An example 2 explains the example which does not have the verification section in this way. Hereafter, in the example 2, although the word verification "routine" is used, the verification section does not exist in this verification routine. That is, the part which judges whether verification was successful does not exist. An access ticket public key (E, n) and the authentication data KE are taken out from the enciphered contents, and the data for authentication are generated using them, it transmits to a certification program, and processing which passes the result of having removed the random-number effectiveness from the certification data returned from the certification program to decode/display, as a decode key is performed.

[0112] Drawing 12 shows the example of a configuration of an example 2. Drawing 12 is the configuration of having lost the verification section 59 from drawing 4 , and is the same configuration as drawing 4 except it.

[0113] Also about actuation, it is almost as the same as the example 1 explained, and [step 1] - [step 7] performs the same processing. Hereafter, [step 8] or subsequent ones is explained.

[0114] [Step 8]: End processing of a verification routine by step 7, and pass a verification routine to decode / display 61 by using as a decode key K' calculated in said random-number effectiveness removal section 58.

[0115] [Step 9]: Decode / display 61 decodes and displays the enciphered contents which separated decode key K' from the random-number effectiveness removal section 58 of a verification routine in reception and the data separation section 56. In a certification program, only when a user with a just token generates certification data using a just access ticket, decode key K' becomes a right decode key, and the enciphered contents are decoded correctly and it is displayed. When a token or an access ticket is not just, decode key K' cannot become a right decode key, and since the enciphered contents are not decoded correctly, it will not be indicated by the right.

[0116] [Example 3] The example 3 of this invention is explained below. Drawing 13 shows the configuration of the example 3 of this invention. The above is an example using a different protocol in a certification data verification side, and this example 3 is close to the configuration which advanced the

component of the verification section shown by drawing 8 (b) of an example 1 out of the verification section. The same number has shown drawing 4 and a corresponding thing. In drawing 13 , 81 expresses the decode key storage section and the verification routine has held the decode key K for decoding contents beforehand.
[0117] The configuration of the enciphered contents consists of an enciphered contents body and an access ticket public key, and does not need to contain authentication data.
[0118] Next, actuation is explained. All the variables in the following explanation are integers.
[0119] [Step 1]: If a user demands use of the contents enciphered from the Internet browser, the Internet browser will look at the data type of the enciphered contents, and will load and start it in search of plug-in related with the data type. If corresponding plug-in starts, the verification routine 15 in plug-in will start. The contents in this case point out what a user uses through the Internet browser, for example, it is the display information on a homepage (an image, an animation, hyper-document, etc.), or they are programs like a Java applet.
[0120] [Step 2]: The verification routine 15 of plug-in takes out an access ticket public key (E, n) from the contents enciphered in the data separation section, and stores it in the access ticket public key storage section 51.
[0121] [Step 3]:, next the verification routine 15 generate a random number r in the random-number generation section 53, store it in the random-number storage section 54, and transmit Challenge C and the number n of access ticket public key methods (the number of the RSA methods) to a certification data generation side by setting a random number r to transmit data (challenge) C. in this case, the certification data which the program for certification returns -- Challenge C -- law -- it should become what is the basis of a number n and was enciphered using RSA cryptograph -- it comes out.
[0122] [Step 4]: In the program for certification, receive Challenge C and the number n of the RSA methods which were sent from the verification routine in the data receive section for authentication, and it is the following, and make and generate the certification data (response) R. First, in the 1st operation part, the access ticket t which uses the number n of the RSA methods as a key, and corresponds is acquired, under the number n of the RSA methods, a formula 6 is performed and middle information R' is obtained from the access ticket storage section 72.
[0123] [step 5]: -- the user proper information e that the 2nd operation part 75 is memorized by the user proper information storage section 74 -- acquiring -- a formula 7 -- performing -- difference -- Information S is acquired.
[0124] [step 6]: and the certification data generation section 76 -- middle information [from the 1st and 2nd operation part 75] R', and difference -- Information S is acquired, a formula 8 is calculated and the certification data R are obtained. The certification data R are transmitted to a verification side.
[0125] [Step 7]: The verification section 59 of the verification routine 15 acquires the received certification data R, and verifies by comparing the random number r and count result r' which calculate a formula 10 and are memorized by the random-number storage section 54.
[0126]
[Equation 10] (10) The r'=RE mod n random number r and count result r' are regarded as verification having been successful, when equal, and the verification routine 15 passes the decode key K to decode/display.
[0127] [Step 8]: Decode / display 61 decodes and displays the enciphered contents which separated the decode key K from the verification section 59 in reception and the data separation section 56. It is more desirable for plug-in to display directly on the field which the Internet browser specified from the field of safety, since the decoded information may be copied by the Internet browser, although the approach of passing the decoded contents to the Internet browser and displaying by the Internet browser is also possible.
[0128] Thus, when it only verifies that a user has a just right and verification is successful, you may make it decode the contents enciphered with the decode key registered beforehand by the verification routine.
[0129] Although the example which constitutes the part of a verification routine from the above 1st

thru/or an example 3 by the software program was shown, the decode key K of contents must be made secret in that case. Because, anyone can decode the contents enciphered as K will be revealed, and they will allow unjust use of contents. Therefore, a verification routine needs to protect an in-house data by a certain approach. As such an approach, in case a program is coded to a machine language, there is the approach of difficulty-in-reading-izing so that it may be hard to analyze an in-house data and a program procedure and they may become. These techniques are introduced by the Takanori Murakami "difficulty-in-reading-ized of program code" Institute of Electronics, Information and Communication Engineers technical research report (IEICE Technical Report) information security, ISEC 95-25 (1995), etc. Moreover, the approach of constituting a verification routine and a decode program from one hardware in addition to the software-based technique may be used. In that case, it can constitute from hardware, a PC card, an IC card of dedication, etc. Moreover, it is also possible to constitute all verification routines, certification data generation sections, and decode/displays from one hardware.
[0130] [Example 4] The example 4 of this invention is explained below. This example explains the example of a configuration which used use control information. Use control information is the control information for controlling generation of certification data, and is control information which describes the conditions which offer service, and is distributed with an access ticket. When not agreeing on conditions, as control information checks these conditions when the term which offers service, a tariff frame, a count, time amount, etc. can be described and certification data are generated, and it does not generate certification data, it can stop offer of service. To control information, the attribute of users, such as an executive, sex, and age, is described besides this, and it is also possible to control generation of certification data as compared with a user's attribute currently held in the token.
[0131] Below, the explanation when using a use term as control information and the explanation when using a tariff frame are described briefly.
[0132] In this example, the access ticket t is data generated based on the following formula 11.
[0133]
[Equation 11]
(11) t=D-F(n,e,L)
the 3 variable function with which, as for the 3 variable function F (x y, z), a function value cannot collide easily -- it is -- for example, the above-mentioned -- on the other hand, it can set like a formula 13 using tropism Hash Function h.
[0134]
[Equation 12]
(12) F(x,y,z)=h(x|y|z)
All the notations in an upper type are integers, like an example 1, the number of the RSA methods and D express an access ticket private key, and, as for e, n expresses user proper information. L is use control information and, on the other hand, function F() is a tropism function.
[0135] With reference to drawing 14 , this example is further explained to a detail. Drawing 14 shows concretely the example of a configuration of the example 4 of this invention. The left half of drawing 14 , i.e., plug-in, and verification routine side is the same as drawing 4 of an example 1.
[0136] The program 32 for certification consists of the data receive section 71 for authentication, the access ticket storage section 72, the 1st operation part 73, and the certification data generation section 76, and a token 33 consists of the user proper information storage section 74, the 2nd operation part 75, and the use control information judging section 77.
[0137] In addition to the number n of the RSA methods, and the access ticket t, the access ticket storage section 72 made use control information L the group, and has memorized it. The use control information judging section 77 passes the use control information L to the 2nd operation part 75, only when the conditions of the use control information L passed from the access ticket storage section 72 are judged and it judges with the right as a result of a judgment. the time of the use control information L being passed from the use control information judging section 77 in the 2nd operation part 75 -- a formula 13 -- being based -- difference -- Information S is calculated and it sends to the certification data generation section 76.

[0138]
[Equation 13]
(13) S=CF (n, e, L) mod The time of using a use term as use control information is explained below by n. When it has a use term as use control information, the value of the use control information L is a value like 199712312400. In this case, this value expresses that a use term is 24:00 on December 31, 1997. It does not matter as for expressing with the relative number of seconds from a certain time instead of such a figure etc.
[0139] The use control information judging section 77 in a token has a clock, and compares with current time of day the use control information L passed from the access ticket storage section 72. And when the value of the use control information L is the back [time of day / current] as a result of a comparison, it judges with the right and the use control information L is passed to the 2nd operation part 75. the time of the use control information L being passed from the use control information judging section 77 in the 2nd operation part 75 -- a formula 13 -- being based -- difference -- Information S is calculated and it sends to the certification data generation section 76.
[0140] Henceforth, like an example 1, the certification data R are calculated using a formula 8 in the certification data generation section 76, in the random-number effectiveness removal section 58 of the verification routine 15, the certification data R received in the certification data receive section 57 are acquired, a formula 9 is calculated with the random number r memorized by the random-number storage section 54, and K' is obtained.
[0141] Whenever count was made using the right access ticket t, the right user proper information e, and the right use control information L, K'=K is realized, the judgment with the right is made by the verification section of the verification routine 15, and service is offered. It is going to use the access ticket with which the use term of the use control information L has expired, and since the access ticket t cannot be altered even if it alters the use control information L it is remembered to be by the access ticket storage section 72 whether you are whom, it cannot become in a right value and the certification data R generated using the formula 8 in the certification data generation section 76 cannot receive offer of service unfairly.
[0142] When the use control information L is the amount of use of service, the figure 100 is given once in 100 yen semantics as a value of for example, the use control information L.
[0143] A token has the prepaid balance storage section which memorizes prepaid balance information, and the use control information judging section 77 in a token compares the use control information L with the prepaid balance, when the prepaid balance is larger, it judges with the right, reduces the value which corresponds in use control information L minutes from the prepaid balance, and passes the use control information L to the 2nd operation part 75. The following processings are the same.
[0144] Moreover, it has the use hysteresis storage section, and the use control information judging section 77 in a token records the value of the use control information L on the use hysteresis storage section with information, such as time of day, and you may make it pass the use control information L to the 2nd operation part 75 instead of the prepaid balance storage section. In this case, it processes collecting the use hysteresis sometimes memorized by the use hysteresis storage section, and paying the corresponding amount of money etc.
[0145] Thus, also except the example shown here, after checking the use control information L by the use control information judging section 77, it becomes possible to perform various use control with constituting so that the use control information L may be passed to the 2nd operation part 75.
[0146] [Example 5] The example 5 of this invention is explained below. An example 5 is an example which distributes the contents encapsulated using satellite broadcasting service, and offers service. Here, it points out preventing from using, if contents are remained as it is by giving encryption etc. as capsulation. The schematic diagram of the service provision system which used satellite broadcasting service for drawing 15 is shown. The encapsulated contents are distributed to each user using satellite broadcasting service. A user receives a satellite electric wave with a satellite antenna, and inputs into a receiver 100. In a receiver, the service provision equipment of this invention is mounted, and when verification is successful, contents can be used.

[0147] The contents offered here can consider various things, such as a movie, music, a TV program, software, a photograph, reference, and news. Each contents are used in the television video 200 connected to the receiver 100, audio equipment 300, and (Computer PC) 400 grade. Here, although the example into which the receiver 100 and the service use device are divided is explained, the service use device by which the receiver 100 was built in can explain similarly.
[0148] The structure of the encapsulated contents is shown in drawing 16 . The encapsulated contents are classified into the data enciphered as the contents header. The contents header has the label, the public key (E, n), and the enciphered decode key for identifying contents. The enciphered data are equivalent to the contents body enciphered in the aforementioned example.
[0149] Drawing 17 is the example which showed the configuration of the receiver 100 in drawing 15 concretely. Each circuit of a receiver 100 is controlled by the microcomputer. The satellite signal from a satellite antenna is first inputted into the tuner 101 of a receiver 100. A tuner 101 extracts the data of the channel which the user chose with the panel of a receiver 100, or remote control. An error correction circuit / descrambling circuit 102 reverts as contents, and inputs the extracted data into the data control circuit 103. In the data control circuit 103, when it identifies with a contents label whether contents are encapsulated or not and contents are not encapsulated in it, an output side is passed as it is. Contents are inputted into verification / decoder circuit 104 when contents are encapsulated. Although it is possible in verification / decoder circuit 104 to verify justification by the verification routine shown in the old example, an example 5 shows and explains an option. The detail of this approach is explained with reference to drawing 18 . In addition, the decoded data are supplied to a use device as a signal which the video decoder 106 or the audio decoder 107 is sent through a demultiplexing circuit 105, and corresponds.
[0150] The verification procedure (protocol) of an example 5 is shown in drawing 18 . The same number has shown the part which has the same function as an example 1.
[0151] The access ticket t in an example 5 is data generated based on a formula 14.
[0152]
[Equation 14] (14) t=D-F(n,e)
All the notations in an upper type are integers, and express the following. (Refer to the formula of an example 1)
n is the product of the number p and q of the RSA methods, i.e., the two sufficiently big prime factors, (n=pq). phi (n) is the Euler number of n, i.e., the product of p-1 and q-1, (phi (n) = (p-1) (q-1)). e expresses user proper information, it is a different number for every user, and it uses it in order to identify a user. D -- an access ticket private key -- expressing -- law -- it is a RSA private key under a number n, and a formula 2 is filled. Here, gcd (x y) expresses the greatest common measure of more than 2 [x] and y.
[0153] The property expressed by the formula (2) guarantees that several E which fills a formula 3 exists. E is called an access ticket public key.
[0154] the 2 variable function with which, as for the 2 variable function F (x y), a function value cannot collide easily -- it is -- for example, the above-mentioned -- on the other hand, it can set like a formula 15 using tropism Hash Function h.
[0155]
[Equation 15]
(15) F(x,y)=h(x|y)
An example 5 is explained to a detail using a Fig. below. The verification / decoder circuit 104 in drawing 17 are shown by 38 at drawing 18 . Verification / decoder circuit 38 consists of a verification routine 15 and the decode section 61, it is realizing by ASIC (application specificintegrated circuit) etc. and the safety of high-speed processing of decode or a verification routine is guaranteed. It is also possible to, realize verification / decoder circuit 38 by the software program, of course. Moreover, in order to raise safety more, you may constitute from hardware which has the Tampa-proof property mentioned above. In verification/decoder circuit, the encapsulated contents which were received from the data control circuit are divided into the data enciphered as the contents header in the data separation

section 56, and the data enciphered by the authentication data storage section 52 in the decode key KE enciphered by the access ticket public key storage section 51 in the public key (E, n) are stored in the decode section 61, respectively. And while verification/decoder circuit generates a random number in the internal random-number generation section and memorizes it in the random-number storage section 54, it calculates transmit data C based on a formula 5 in the transmit data count section like an example 1.
[0156] thus, calculated transmit data C -- law -- it is transmitted to a certification program together with a number n.
[0157] The operation of the 1st operation part 73 of a certification program and the certification data generation section 76 is performed with a microcomputer, and the access ticket is memorized by EPROM (erasableprogrammable read only memory) etc. Authentication data choose the access ticket [/ based on n which received] t, it is the basis of the number n of the RSA methods received from the authentication data receive section 71, and perform a formula 16 and obtain middle information R' from the access ticket storage section 72.
[0158]
[Equation 16]
(16) R'=Ct mod an IC card realizes n token -- having -- the user proper information storage section 74 and the 2nd operation part 75 -- having -- a microcomputer to the data for authentication -- receiving -- a formula 17 -- performing -- difference -- Information S is acquired.
[0159]
[Equation 17]
(17) S=CF (n, e) mod n and the certification data generation section 75 of a certification program -- middle information [from the 1st and 2nd operation part 73 and 75] R', and difference -- Information S is acquired, a formula 18 is calculated and the certification data R are obtained.
[0160]
[Equation 18] (18) R=R'S mod n, thus the obtained certification data R are transmitted to the certification data receive section 57 of verification/decoder circuit.
[0161] The random-number effectiveness removal section 58 of the verification routine 15 acquires the certification data R received in the data receive section 57, calculates a formula 19 with the random number r memorized by the random-number storage section 54, and obtains the decode key K.
[0162]
[Equation 19] (19) K=Rr -1 mod n -- redundancy is given to K at this time and you may make it verify whether the decode key K was correctly decoded by giving a specific value to that part in the verification section 59 The obtained decode key K is inputted into the decode section 61, in the decode section 61, decodes the enciphered data using the decode key K, and outputs them as contents.
[0163] The outputted contents are used with PC as digital data, or are used as image information or audio information.
[0164] The general-view Fig. of the service provision equipment of this example is shown in drawing 19 . As shown in drawing, service provision equipment is connected to television. Although not shown in drawing, while it connects with the satellite antenna and service provision equipment receives satellite broadcasting service, it connects with the network through the modem and it can acquire the access ticket for using the encapsulated contents which received by satellite broadcasting service. As shown in drawing 19 (a), when contents are enciphered and the token is not being inserted in service provision equipment, a user cannot see an image. Then, if a user acquires a just access ticket and a token is inserted in service provision equipment, as shown in drawing 19 (b), he can see an image.
[0165] Thus, in this invention, in spite of enciphering and offering contents by one cryptographic key, if it does not have both of tokens which stored the access ticket customized for every user, and user proper information, service can be used no longer. Therefore, contents are enciphered, and the provider (provider) of contents can be provided using the mass media like satellite broadcasting service, and can perform positive use management for every user by the access ticket and the token.
[0166] [Example 6] The example 6 of this invention is explained below. Although the above described

the case where it encapsulated for every contents, the encryption same about the broadcast channel of satellite broadcasting service is given as applications other than this, and there is a case where he wants to restrict use of contents by managing viewing-and-listening time amount etc. Such service is realized by expressing an access ticket by the formula 20.
[0167]
[Equation 20] (20) t=D-F(n,e,L)
Here, L is use control information and expresses a use term. the 3 variable function with which, as for the 3 variable function F (x y, z), a function value cannot collide easily -- it is -- for example, the above-mentioned -- on the other hand, it can set like a formula 21 using tropism Hash Function h.
[0168]
[Equation 21]
(21) F(x,y,z)=h(x|y|z)
The example of a configuration of use control information is shown in drawing 20. The use control information L consists of use start time, use end time, and a use tariff as shown in drawing. A use tariff is required only when a token has a prepaid function, and when not using a prepaid function, it can be omitted. The verification protocol at the time of using the use control information L for drawing 21 is shown. The same number has shown the thing of the same function as drawing 18 here.
[0169] Hereafter, an example 6 is explained to a detail using drawing. In verification/decoder circuit, the encapsulated contents which were received from the data control circuit are divided into the data enciphered as the contents header in the data separation section 56, and the data enciphered by the authentication data storage section 52 in the decode key KE enciphered by the access ticket public key storage section 51 in the public key (E, n) are stored in the decode section 61, respectively. And while verification/decoder circuit generates a random number in the internal random-number generation section and memorizes it in the random-number storage section 54, it calculates transmit data C based on a formula 15 in the transmit data count section.
[0170] thus, calculated transmit data C -- law -- it is transmitted to a certification program together with a number n.
[0171] The operation of the 1st operation part 73 of a certification program and the certification data generation section 76 is performed with a microcomputer, and the access ticket is memorized by EPROM (erasableprogrammable read only memory) etc. Authentication data choose the access ticket t and the use control information L, it is the basis of the number n of the RSA methods received from the authentication data receive section 71, and perform a formula 16 and obtain middle information R' from the access ticket storage section 72. [/ based on n which received]
[0172] A token has the user proper information storage section 74 and the 2nd operation part 75, and has prepaid frequency and token time-of-day data further. A token verifies whether the expiration date in reception and use control information is contradictory to token time of day in the data for authentication, and the use control information L from a microcomputer. That is, when use start time <= token time-of-day <= use end time has come, it is considered that verification was successful. If it succeeds in verification of an expiration date, it checks that the frequency of a token remains more than the number of availabilities within the use control information L, and if it remains, several availability minutes in the use control information L will be subtracted from the frequency of a token. When verification of an expiration date went wrong, and when frequency is insufficient, it does not process but an error is returned. the case where the above-mentioned verification is successful -- a formula 22 -- performing -- difference -- Information S is acquired.
[0173]
[Equation 22]
(22) S=CF (n, e, L) mod n and the certification data generation section 75 of a certification program -- middle information [from the 1st and 2nd operation part 73 and 75] R', and difference -- Information S is acquired, a formula 18 is calculated and the certification data R are obtained. Thus, the obtained certification data R are transmitted to the certification data receive section 57 of verification/decoder circuit.

[0174] The random-number effectiveness removal section 58 of the verification routine 15 acquires the certification data R received in the data receive section 57, calculates a formula 19 with the random number r memorized by the random-number storage section 54, and obtains the decode key K. Here, when the use control information L used by the token is altered, an exact decode key cannot be taken out. Redundancy is given to K at this time and you may make it verify whether the decode key K was correctly decoded by giving a specific value to that part in the verification section 59. The obtained decode key K is inputted into the decode section 61, in the decode section 61, decodes the enciphered data using the decode key K, and outputs them as contents.
[0175] The outputted contents are used with PC as digital data, or are used as image information or audio information.
[0176] In this example, although time of day is given to the token, since there is no clock in the interior when using an IC card, it is necessary to guarantee the justification of token time of day.
[0177] It is also possible to be able to set up the right of use for every time amount, and to realize functions, such as pay-per-view, by doing in this way, though he cannot use an access ticket unless a user is within the expiration date in use control information, but the contents of one channel are enciphered by the same cryptographic key.
[0178] In addition, this invention is not limited to an above-mentioned example, and use of contents can be performed through various record media, communication media, and a broadcast medium. It can apply, when using the various communication media and the broadcast medium other than the Internet and satellite broadcasting service. For example, it is applicable also to offer of service of the online karaoke by the usual telephone network, the data communication network, and TCP/IP connection.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the block diagram showing the theoretic example of a configuration of this invention.
[Drawing 2] It is the block diagram showing the outline of the example of a configuration of an example 1.
[Drawing 3] It is the schematic diagram of the computer which the user of an example 1 uses.
[Drawing 4] It is the detailed block diagram of the example of a configuration of an example 1.
[Drawing 5] It is the example 1 of a configuration of the contents as which the example 1 was enciphered.
[Drawing 6] It is the example 2 of a configuration of the contents as which the example 1 was enciphered.
[Drawing 7] It is the example 3 of a configuration of the contents as which the example 1 was enciphered.
[Drawing 8] It is the example of a configuration of the processing in the verification section of an example 1.
[Drawing 9] It is the example of a configuration of the processing in the verification section of an example 1.
[Drawing 10] It is the example of a configuration of the processing in the verification section of an example 1.
[Drawing 11] It is the example of a configuration of the processing in the verification section of an example 1.
[Drawing 12] It is the detailed block diagram of the example of a configuration of an example 2.
[Drawing 13] It is the detailed block diagram of the example of a configuration of an example 3.
[Drawing 14] It is the detailed block diagram of the example of a configuration of an example 4.
[Drawing 15] It is the schematic diagram of an example 5.
[Drawing 16] It is the block diagram of contents with which the example 5 was encapsulated.
[Drawing 17] It is the detailed block diagram of the example of a configuration of an example 5.
[Drawing 18] It is the detailed block diagram of the example of a configuration of an example 5.
[Drawing 19] It is drawing of the example of a configuration of an example 5.
[Drawing 20] It is the block diagram of the use control information of an example 6.
[Drawing 21] It is the detailed block diagram of the example of a configuration of an example 6.
[Description of Notations]
10 Certification Data Verification Equipment
11 Certification Data Generation Equipment
12 Access Ticket Generation Equipment
13 Access Ticket (Auxiliary Data for Certification)
14 The Description Information on Access Rating Authentication
15 Verification Routine
16 User Proper Information

17 Certification Data Generator
18 Data for Authentication
19 Certification Data
20 Tamper-proof Equipment
30 Computer
31 Internet Browser
32 Program for Certification
33 Token
34 Contents
35 Decode Program
38 Plug-in (Plug-in Module)

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－31130

(43)公開日　平成11年(1999)２月２日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｂ

審査請求　未請求　請求項の数21　ＯＬ　（全 44 頁）

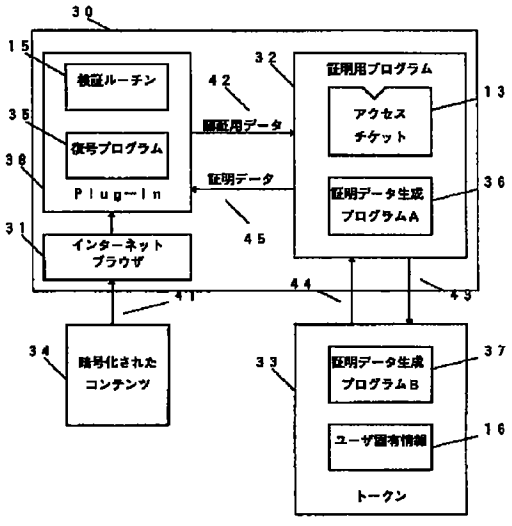
(21)出願番号　特願平9－184866

(22)出願日　平成９年(1997)７月10日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号
(72)発明者　河野　健二
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内
(72)発明者　中垣　寿平
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内
(72)発明者　小島　俊一
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内
(74)代理人　弁理士　澤田　俊夫

(54)【発明の名称】　サービス提供装置

(57)【要約】
【課題】　ユーザおよびサービス提供者の負担を最小限に押さえながら、サービスの利用を正当な権利を有するユーザにのみ提供する。
【解決手段】　インターネットブラウザ３１のプラグイン３８が起動すると、プラグイン３８中の検証プログラム１５が起動し、証明用プログラム３２と通信してユーザ認証を行う。証明用プログラム３２の証明データ生成プログラムＡ３６は、トークン３３中の証明データ生成プログラムＢ３７と協調して、ユーザ固有情報１６とアクセスチケット１３とに基づいて計算を行い、その計算に基づいてプラグイン３８中の検証プログラム１５と通信を行う。通信の結果、検証プログラム１５による認証が成功するのは、ユーザ固有情報と、アクセスチケットと、暗号化されたコンテンツとの３つが正しく対応している場合に限られる。



1

【特許請求の範囲】

【請求項１】　正当な権利を有するユーザのみにサービスを提供するサービス提供装置において、
認証用データを記憶する第１の記憶手段と、
ユーザの固有情報を記憶する第２の記憶手段と、
前記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第３の記憶手段と、
前記第１の記憶手段に保持されている認証用データと、前記第２の記憶手段に記憶されている前記ユーザの固有情報と、前記第３の記憶手段に記憶されている前記証明用補助情報とに所定の計算を施して証明データを生成する証明データ生成手段とを有し、
前記証明データ生成手段によって生成された証明データを利用してサービスを提供することを特徴とするサービス提供装置。

【請求項２】　正当な権利を有するユーザのみにサービスを提供するサービス提供装置において、
認証用データを記憶する第１の記憶手段と、
ユーザの固有情報を記憶する第２の記憶手段と、
前記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第３の記憶手段と、
前記第１の記憶手段に保持されている認証用データと、前記第２の記憶手段に記憶されている前記ユーザの固有情報と、前記第３の記憶手段に記憶されている前記証明用補助情報とに所定の計算を施して証明データを生成する証明データ生成手段と、
前記証明データ生成手段によって生成された証明データが前記アクセス資格認証の特徴情報に基づいて生成されていることを検証する証明データ検証手段とを有し、
前記証明データ検証手段による検証が成功した場合にのみ、サービスを提供することを特徴とするサービス提供装置。

【請求項３】　利用を制限された情報を入力する入力手段を更に有し、
前記証明データ検証手段による検証が成功した場合にのみ、前記情報に対する利用の制限を解除して情報の利用を可能にすることを特徴とする請求項２に記載のサービス提供装置。

【請求項４】　前記アクセス資格認証の特徴情報が暗号化関数における復号鍵であり、前記認証用データが適当なデータを前記復号鍵に対応する暗号化鍵を用いて暗号化したものであり、
前記証明データ検証手段は、前記証明データ生成手段が生成する証明データが前記認証用データを正しく復号したものである場合に検証が成功したと判定することを特徴とする請求項２または３に記載のサービス提供装置。

【請求項５】　前記アクセス資格認証の特徴情報が暗号化関数における暗号化鍵であり、

2

前記証明データ検証手段は、前記証明データ生成手段が生成する証明データが前記認証用データを正しく暗号化したものである場合に検証が成功したと判定することを特徴とする請求項２または３に記載のサービス提供装置。

【請求項６】　前記アクセス資格認証の特徴情報は、デジタル署名関数における署名鍵であり、前記証明データ検証手段は、前記証明データ生成手段が生成する証明データが、前記認証用データに対して、前記署名鍵を用いて正しく生成されたデジタル署名であることが検証された場合に検証が成功したと判定することを特徴とする請求項２または３に記載のサービス提供装置。

【請求項７】　前記利用を制限された情報は、少なくとも一部が暗号化された情報であり、
前記証明データ検証手段による検証が成功した場合にのみ、前記暗号化された情報を復号して情報の利用を可能にすることを特徴とする請求項２乃至６に記載のサービス提供装置。

【請求項８】　暗号化された情報を入力する入力手段を更に有し、
前記アクセス資格認証の特徴情報が暗号化関数における第１の復号鍵であり、前記認証用データが前記暗号化された情報を復号する第２の復号鍵を前記第１の復号鍵に対応する暗号化鍵を用いて暗号化したものであり、
前記証明データ生成手段によって生成された証明データが前記第２の復号鍵であり、前記第２の復号鍵を用いて前記暗号化された情報を復号して、前記情報に対応するサービスを提供することを特徴とする請求項１または２に記載のサービス提供装置。

【請求項９】　前記暗号化関数が非対称鍵暗号化関数であり、前記アクセス資格認証の特徴情報が鍵の一方であることを特徴とする請求項４、５または８に記載のサービス提供装置。

【請求項１０】　前記暗号化関数が公開鍵暗号化関数であり、前記アクセス資格認証の特徴情報が秘密鍵であることを特徴とする請求項４、５または８に記載のサービス提供装置。

【請求項１１】　前記暗号化関数が対称鍵暗号化関数であり、前記アクセス資格認証の特徴情報が共通秘密鍵であることを特徴とする請求項４、５または８に記載のサービス提供装置。

【請求項１２】　証明データ生成装置および証明データ検証装置を具備し、前記証明データ生成装置および前記証明データ検証装置が通信を行ってユーザのアクセス資格を認証するアクセス資格認証装置を有するサービス提供装置において、
前記証明データ生成装置は、
認証用データを記憶する第１の記憶手段と、
ユーザの固有情報を記憶する第２の記憶手段と、
前記ユーザの固有情報と、アクセス資格認証の特徴情報

とに対して、所定の計算を実行した実行結果である証明用補助情報を記憶する第３の記憶手段と、
前記第１の記憶手段に保持されている前記認証用データと、前記第２の記憶手段に保持されている前記ユーザの固有情報と、前記第３の記憶手段に保持されている前記証明用補助情報とに所定の計算を実行して証明情報を生成する証明データ生成手段とを有し、
前記証明データ検証装置は、
認証用データを記憶する第４の記憶手段と、
証明データを記憶する第５の記憶手段と、
前記証明データ生成手段によって生成された前記証明データが前記アクセス資格認証用の特徴情報に基づいて生成されていることを検証する証明データ検証手段とを有し、
前記証明データ検証装置は、前記第４の記憶手段に記憶されている前記認証用データを前記証明データ生成装置の前記第１の記憶手段に書き出し、
前記証明データ生成装置は、前記証明データ生成手段によって前記第１の記憶手段に書き込まれた前記認証用データをもとに生成した前記証明データを、前記証明データ検証装置の前記第５の記憶手段に書き出し、
前記証明データ検証装置は前記第５の記憶手段に書き込まれた前記証明データを用いてユーザのアクセス資格を認証することを特徴とするサービス提供装置。
【請求項１３】　前記アクセス資格認証用の特徴情報が暗号化関数の復号鍵であり、
前記証明データ検証装置が乱数生成手段と、生成した乱数を記憶する第６の記憶手段と、認証用素データを記憶する第７の記憶手段とを備え、
前記乱数生成手段は生成した乱数を前記第６の記憶手段に書き込むと共に、前記第７の記憶手段に記憶されている前記認証用素データに前記乱数を用いた乱数効果を施した後、前記認証用データとして前記第４の記憶手段に書き込み、
前記証明データ検証手段は、前記第６の記憶手段に記憶されている前記乱数による乱数効果を、前記証明データ生成装置によって前記第５の記憶手段に書き込まれた前記証明データから除去した結果が、前記アクセス資格認証の特徴情報である復号鍵で前記第７の記憶手段に記憶されている前記認証用素データを復号したものであることを検証することを特徴とする請求項１２に記載のサービス提供装置。
【請求項１４】　前記アクセス資格認証用の特徴情報が暗号化関数の暗号化鍵であり、
前記証明データ検証装置が乱数生成手段を備え、前記乱数生成手段は生成した乱数を前記認証用データとして前記第４の記憶手段に書き込み、
前記証明データ検証手段は、前記証明データ生成装置によって前記第５の記憶手段に書き込まれた前記証明データが、前記乱数を復号したものであることを検証することを特徴とする請求項１２に記載のサービス提供装置。

【請求項１５】　前記アクセス資格認証用の特徴情報がデジタル署名関数の署名鍵であり、
前記証明データ検証装置が乱数生成手段を備え、前記乱数生成手段は生成した乱数を認証用データとして前記第４の記憶手段に書き込み、
前記証明データ検証手段は、前記証明データ生成装置によって前記第５の記憶手段に書き込まれた前記証明データが、前記乱数である認証用データに対する、前記アクセス資格認証の特徴情報である署名鍵によるデジタル署名であることを検証することを特徴とする請求項１２に記載のサービス提供装置。
【請求項１６】　少なくとも、前記第２の記憶手段と、前記証明データ生成手段とが、内部データおよび処理手続きを外部から観測することを困難ならしめる防御手段中に保存されていることを特徴とする請求項１乃至１５に記載のサービス提供装置。
【請求項１７】　少なくとも、前記第２の記憶手段と、前記証明データ生成手段とが、ＩＣカードなどの携帯可能な小型演算装置として構成されていることを特徴とする請求項１乃至１５に記載のサービス提供装置。
【請求項１８】　少なくとも、前記証明データ検証手段が、内部データおよび処理手続きを外部から観測することを困難ならしめる防御手段中に保存されていることを特徴とする請求項１乃至１５に記載のサービス提供装置。
【請求項１９】　少なくとも、前記証明データ検証手段が、ＩＣカードなどの携帯可能な小型演算装置として構成されていることを特徴とする請求項１乃至１５に記載のサービス提供装置。
【請求項２０】　前記入力手段から入力される情報は、イメージ、動画、音声、音楽などのマルチメディア情報または前記マルチメディアを暗号化したものであり、
前記サービスは、前記入力された情報を再生することを特徴とする請求項１乃至１９に記載のサービス提供装置。
【請求項２１】　前記証明データの生成を制御する利用制御情報を記憶する第８の記憶手段をさらに有し、
前記第３の記憶手段に保持されている前記証明用補助情報は、前記ユーザの固有情報と、前記アクセス資格認証の特徴情報と、前記利用制御情報とに対し、所定の計算を実行した実行結果であり、
前記証明データ生成手段は、前記第１の記憶手段に保持されている認証用データと、前記第２の記憶手段に記憶されている前記ユーザの固有情報と、前記第３の記憶手段に記憶されている前記証明用補助情報と、前記第８の記憶手段に記憶されている前記利用制御情報とに所定の計算を施して証明データを生成することを特徴とする請求項１乃至２０に記載のサービス提供装置。
【発明の詳細な説明】

5

【０００１】
【発明の属する技術分野】本発明は、正当な権利を有するユーザにのみ選択的にサービスを提供することのできるサービス提供装置およびその方法に関する。
【０００２】
【従来技術】近年のネットワークの発達によって、さまざまな情報がディジタル化されネットワークを通じて流通する時代が到来している。ディジタル化される情報としては、文字情報をはじめ静止画、動画、音声、プログラムなどがあり、我々はネットワーク上でこれらを組み合わせたさまざまなサービスを受けることが可能である。しかし、これらディジタル情報の大きな特徴であるコピーの容易性が、これまでネットワークでのディジタル情報の流通を阻害する要因となっていた。これは、ディジタル情報をコピーするとオリジナルとまったく同じ物を生成することができるため、一旦流通したものが著作者の意図しないところで無断で使用され、著作者が得るべき正当な対価を回収し難いという問題に起因する。
【０００３】この問題を解決するため、最近では日本アイ・ビー・エム（株）のＣＤ－ＳＨＯＷＣＡＳＥ（商標または製品名）のように、ディジタル情報を暗号化して自由に流通させ、利用する際には代金を支払って電話回線等で復号鍵を受け取り、ディジタル情報を利用するようなシステムも登場している。また、特公平６－９５３０２号公報の「ソフトウエア管理方式」には、ソフトウエアを利用した量に応じて課金し料金を回収するシステムの例が示されている。特公平７－２１２７６号公報の「情報利用量測定装置」では、放送によって配布された情報のすべての利用者の情報利用時間等の利用量を的確に測定することができる情報利用量測定装置について述べられている。これによると情報利用量測定装置は、暗号化された書籍情報を受信し蓄積し、ユーザが書籍情報を復号し表示した時間と量を利用履歴として記録しておきそれにより料金を徴収する例が示されている。
【０００４】前記のシステムを実現する方法として、さまざまな暗号技術やプログラムの実行制御技術が先行技術として知られている。
【０００５】プログラム実行制御技術は、
①アプリケーションプログラム中に、ユーザのアクセス資格認証のためのルーチンを埋め込み、
②該ルーチンはアプリケーションの実行を試みているユーザが正規の認証用の鍵を保有していることを検査し、
③前記認証用の鍵の存在が確認された場合に限りプログラムを続行し、それ以外の場合はプログラムの実行を停止する
技術である。当技術を利用することにより、認証鍵を保有する正規のユーザのみアプリケーションの実行を可能ならしめることができる。当技術は、ソフトウエア領布事業において実用化されており、製品としては、例えばＲａｉｎｂｏｗＴｅｃｈｎｏｌｏｇｉｅｓ，　Ｉｎｃ．

6

社のＳｅｎｔｉｎｅｌ　ＳｕｐｅｒＰｒｏ（商標）や、Ａｌａｄｄｉｎ　Ｋｎｏｗｌｅｄｇｅ　Ｓｙｓｔｅｍｓ　Ｌｔｄ．社のＨＡＳＰ（商標）等がある。
【０００６】以下にプログラム実行制御技術についてより詳細に説明する。
①ソフトウエアの実行を行うユーザはユーザ固有情報として認証鍵を保有する。認証鍵は暗号化のための鍵であり、ソフトウエアの利用を許可する者、例えばソフトウエアベンダーがユーザに配布する。認証鍵は複製を防ぐためにハードウエア中のメモリに厳重に封入され、郵便等の物理的手段を用いてユーザに配送される。
②ユーザ認証鍵を内蔵したハードウエアを指定された方法で所有者のパソコンまたはワークステーションに装着する。ハードウエアは例えばプリンタポート等に装着される。
③ユーザがアプリケーションプログラムを起動し、プログラムの実行が前記アクセス資格認証ルーチンに及ぶと、プログラムはユーザの認証鍵を内蔵したハードウエアと通信する。通信結果に基づいてプログラムは認証鍵を識別し、正しい認証鍵の存在が確認されると次のステップへ実行を移す。通信が失敗し認証鍵の存在が確認されない場合は、プログラムは自らを停止し以降の実行ができないようにする。
【０００７】アクセス資格認証ルーチンによる認証鍵の識別は、例えば次のようなプロトコルによって行われる。
①アクセス資格認証ルーチンは適当な数を生成し鍵内蔵ハードウエアに送信する。
②鍵内蔵ハードウエアは内蔵する認証鍵を用いて送られた数を暗号化し、前記アクセス資格認証ルーチンに返信する。
③認証ルーチンは、返信された数が予め予想された数、即ちハードウエアに送信した数を正しい認証鍵で暗号化して得られる数であるか否かを判定する。
④返信された数が予想された数と一致する場合にはプログラムの実行を継続し、一致しない場合にはプログラムを停止する。
【０００８】この際のアプリケーションプログラムと認証鍵内蔵ハードウエア間の通信は、たとえ同じアプリケーションプログラム中の同じ箇所において同じハードウエアとの間で交換されるものであろうとも、実行のたびに異ならなければならない。さもなければ、正常な実行過程における通信内容を一度記録し、以後プログラムを実行するたびに記録した通信内容をアプリケーションプログラムに返信することにより、正しい認証鍵を保有しないユーザでもプログラムを実行することが可能となってしまう。このような攻撃をリプレイアタックと呼ぶ。
【０００９】リプレイアタックを防ぐために、通常鍵内蔵ハードウエアに送られる数は通信のたびに新たに生成される乱数を用いる。

【００１０】［従来技術の問題点］従来技術の問題点は、アプリケーションプログラムを作成する際に、プログラム作成者がユーザが持つ認証鍵を予め想定した上で、該認証鍵に基づいてプログラムの保護処理を行わなければならないという性質に由来する。

【００１１】つまり、プログラムの作成者は、鍵内蔵ハードウエアからの正しい返信をプログラム作成時に予側して、正しい返信を受けた場合にのみプログラムが正常に実行されるようにプログラムの作成を行わなければならない。

【００１２】前記の特徴を有する従来技術の利用形態は基本的に前記の二通りとなるが、いずれの場合も以下に述べる問題を有する。

【００１３】①第１の方法では、ユーザの認証鍵をユーザ毎に異なるように用意する。即ち、ユーザ甲には認証鍵甲、ユーザ乙には認証鍵乙というように、ユーザごとに異なる認証鍵を１つずつ用意する。この場合、プログラム中の認証ルーチンは該プログラムを利用するユーザの固有の認証鍵を認証できるように作成されなければならず、プログラム作成者は利用ユーザの数だけ異なるプログラムを作成する必要がある。

【００１４】対象となるユーザが多数の場合、プログラムをユーザ毎にカスタマイズ（個別化）する作業はプログラム作成者にとって耐え難い労力を要求し、管理しなければならないユーザ認証鍵のリストも膨大なものとなる。

【００１５】②第２の方法では、プログラムの作成者はアプリケーションごとにそれぞれ異なる認証鍵を用意する。即ち、アプリケーション甲には認証鍵甲、アプリケーション乙には認証鍵乙というように、アプリケーションごとに異なる認証鍵を１つずつ用意し、固有の認証鍵を識別するように各アプリケーションプログラムを作成する。

【００１６】この方法では、第１の方法のようにユーザ毎にプログラムを個別的に作成する必要はなくなるが、逆にユーザは利用するアプリケーションの数だけ認証鍵を保持しなければならないことになる。

【００１７】上述のように、認証鍵はハードウエアに厳重に封入した状態でユーザに配布する必要がある。従って、プログラム自身はネットワークを介して簡便に配布することができるのに対し、認証鍵を内蔵するハードウエアの配布は郵便等の物理的手段に頼らざるを得ない。プログラム作成者はユーザからのアプリケーションの使用許諾以来を上け取るたびに、そのアプリケーションに対応する認証鍵が封入されたハードウエアを郵送する必要があり、コスト、時間、梱包の手間いずれをとってもプログラム作成者にとって大きな負担となる。

【００１８】また、ユーザは利用するアプリケーションを変更するたびにハードウエアを交換しなければならないという煩雑さに甘んじなければならない。

【００１９】ユーザがあるアプリケーションを使いたいとしても、認証鍵が封入されたハードウエアが郵送されて到着するまで待たなければならず、即座に利用できないという問題もある。

【００２０】これら問題を軽減するために、ハードウエア中に予め複数の認証鍵を封入しておき、新しいアプリケーションの利用をユーザに許可するたびに、ハードウエア中の認証鍵を利用可能とするためのパスワードをユーザに教えるという方法を用いることはできるが、予め封入された認証鍵を使い切った場合は同様の問題が発生し、本質的な解決とはなっていない。

【００２１】前記のような実効制御の方法以外に、単にアプリケーションを暗号化して、その復号鍵を安全な方法でユーザに教えるという単純な方法が一般的に広く用いられているが、この方法では、アプリケーションを一旦復号してしまうと、ユーザは好きなようにアプリケーションをコピーして不正に配ることができるため、ほとんど防御されていないとみなしてよい。

【００２２】従って、デジタル化された情報、例えばソフトウエア、音楽、映画等（以後これらを総称してコンテンツと呼ぶ）をネットワークで配送して、正当な対価を得ようとした場合、従来の技術では、コンテンツの管理が煩雑になったり、認証用のハードウエアの管理でユーザに大きな負担をかけてしまうという問題があった。

【００２３】

【発明が解決しようとする課題】本発明は、このような問題に鑑みなされたものであり、ユーザおよびサービス提供者の負担を最小限に押さえながら、サービスの利用を正当な権利を有するユーザにのみ提供することができるシステム、または、サービスの利用に応じた正当な対価を回収することが可能なシステムを提供することを目的とする。

【００２４】

【課題を解決するための手段】本発明の第１の側面によれば、上述の目的を達成するために、正当な権利を有するユーザのみにサービスを提供するサービス提供装置に、認証用データを記憶する第１の記憶手段と、ユーザの固有情報を記憶する第２の記憶手段と、前記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第３の記憶手段と、前記第１の記憶手段に保持されている認証用データと、前記第２の記憶手段に記憶されている前記ユーザの固有情報と、前記第３の記憶手段に記憶されている前記証明用補助情報とに所定の計算を施して証明データを生成する証明データ生成手段とを設けるようにしている。

【００２５】また、本発明の第２の側面によれば、正当な権利を有するユーザのみにサービスを提供するサービス提供装置に、認証用データを記憶する第１の記憶手段と、ユーザの固有情報を記憶する第２の記憶手段と、前

記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第３の記憶手段と、前記第１の記憶手段に保持されている認証用データと、前記第２の記憶手段に記憶されている前記ユーザの固有情報と、前記第３の記憶手段に記憶されている前記証明用補助情報とに所定の計算を施して証明データを生成する証明データ生成手段と、前記証明データ生成手段によって生成された証明データが前記アクセス資格認証の特徴情報に基づいて生成されていることを検証する証明データ検証手段とを設けるようにしている。

【００２６】これらの構成によれば、証明用補助データ（アクセスチケット）を導入することにより、プロテクト側で付与されるアクセス資格認証用の特徴情報とユーザ側に付与されるユーザ固有情報とを独立させることができ、ユーザは予めユーザ固有情報を所持し、プログラム作成者等のプロテクト者はユーザが所持するユーザ固有情報とは独立にアクセス資格認証の特徴情報を用いてアプリケーションプログラムを作成し、その後、アクセスチケットをユーザの個有情報とアプリケーションプログラムの作成等に使用したアクセスチケット資格認証の特徴情報とに応じて作成し、配布することにより、実行制御等のユーザアクセス資格の認証を行うことが可能となり、正当な権利を有するユーザにのみ所望のサービスを提供することができる。また、証明データ生成時にログを取るようにすれば、サービスに対する正当な対価を回収することができる。

【００２７】また、前記の構成においては、少なくとも前記第２の記憶手段と、前記証明データ生成手段とが、内部データおよび処理手続きを外部から観測することが困難ならしめる防御手段中に保持されるようにしてもよい。

【００２８】また、前記の構成においては、少なくとも前記証明データ検証手段が、内部データおよび処理手続きを外部から観測することが困難ならしめる防御手段中に保持されるようにしてもよい。

【００２９】また、前記アクセス資格認証の特徴情報が暗号化関数における復号鍵であり、前記認証用データが適当なデータを前記復号鍵に対応する暗号化鍵を用いて暗号化したものであり、前記証明データ検証手段により、前記証明データ生成手段が生成する証明データが前記認証用データを正しく復号したものであることを検証するようにしてもよい。また、前記アクセス資格認証の特徴情報が暗号化関数における暗号化鍵であり、前記認証用データが適当なデータを前記暗号化鍵に対応する復号鍵を用いて復号したものであり、前記証明データ検証手段により、前記証明データ生成手段が生成する証明データが前記認証用データを正しく暗号化したものであることを検証するようにしてもよい。また、前記アクセス資格認証の特徴情報がデジタル署名関数における署名鍵であり、前記証明データ生成手段が生成する証明データが、前記認証用データに対して、前記署名鍵を用いて正しく生成されたデジタル署名であることを検証するようにしてもよい。

【００３０】また、前記アクセス資格認証の特徴情報が暗号化関数における第１の復号鍵であり、前記認証用データが前記暗号化された情報を復号する第２の復号鍵を前記第１の復号鍵に対応する暗号化鍵を用いて暗号化したものであり、前記証明データ生成手段によって生成された証明データが前記第２の復号鍵であり、前記第２の復号鍵を用いて前記暗号化された情報を復号して、前記情報に対応するサービスを提供するようにしてもよい。また、前記暗号化関数が非対称鍵暗号化関数であり、アクセス資格認証の特徴情報が鍵の一方であってもよい。

【００３１】また、前記暗号化関数が公開鍵暗号化関数であり、アクセス資格認証の特徴情報が秘密鍵であってもよい。

【００３２】また、前記暗号化関数が対称鍵暗号化関数であり、アクセス資格認証の特徴情報が共通秘密鍵であってもよい。

【００３３】また、前記第１の記憶手段と、前記第２の記憶手段と、前記第３の記憶手段と、前記証明データ生成手段とから構成される証明データ生成装置と、前記証明データ検証手段に加え、認証用データを記憶する第４の記憶手段と、証明データを記憶する第５の記憶手段をそなえた証明データ検証装置とが、互いに通信することによりユーザのアクセス資格を認証するアクセス資格認証装置を有するサービス提供装置において、証明データ検証装置は、第４の記憶手段に記憶されている認証用データを証明データ生成装置の第１の記憶手段に書き出し、証明データ生成装置は、証明データ生成手段によって第１の記憶手段に書き込まれた前記認証用データをもとに生成した証明データを、証明データ検証装置中の第５の記憶手段にかき出し、証明データ検証装置は第５の記憶手段に書き込まれた前記証明データを用いてユーザのアクセス資格を認証するようにすることもできる。

【００３４】また、アクセス資格認証用の特徴情報が暗号化関数の復号鍵であり、証明データ検証装置が乱数生成手段と、生成した乱数を記憶する第６の記憶手段と、認証用素データを記憶する第７の記憶手段とを備え、乱数生成手段は生成した乱数を第６の記憶手段に書き込むと共に、第７の記憶手段に記憶されている認証用素データに前記乱数を用いた乱数効果を施した後、認証用データとして第４の記憶手段に書き込み、証明データ検証手段は、第６の記憶手段に記憶されている乱数による乱数効果を、前記証明データ生成装置によって第５の記憶手段に書き込まれた証明データから除去した結果が、アクセス資格認証の特徴情報である復号鍵で第７の記憶手段に記憶されている認証用素データを復号したものであることを検証するようにしてもよい。

【００３５】また、アクセス資格認証用の特徴情報が暗号化関数の暗号化鍵であり、証明データ検証装置が乱数生成手段を備え、乱数生成手段は生成した乱数を認証用データとして第４の記憶手段に書き込み、証明データ検証手段は、証明データ生成装置によって第５の記憶手段に書き込まれた証明データが、前記乱数を復号したものであることを検証するようにしてもよい。

【００３６】また、アクセス資格認証用の特徴情報がデジタル署名関数の署名鍵であり、証明データ検証装置が乱数生成手段を備え、乱数生成手段は生成した乱数を認証用データとして第４の記憶手段に書き込み、証明データ検証手段は、証明データ生成装置によって第５の記憶手段に書き込まれた証明データが、前記乱数である認証用データに対する、アクセス資格認証の特徴情報である署名鍵によるデジタル署名であることを検証するようにしてもよい。

【００３７】

【発明の実施の態様】以下、この発明を詳細に説明する。

［実施例１］まず、実施例１を参照して本発明の原理的な構成について説明する。図１は本発明の実施例１の構成を全体として示すものであり、この図１においてサービス提供システムは、証明データ検証装置１０および証明データ生成装置１１からなっており、証明データ生成装置１１はアクセスチケット生成装置１２からアクセスチケット（証明用補助データ）１３を受領するようになっている。証明データ検証装置１０は検証ルーチン１５を実行する。証明データ生成装置１１はユーザ固有情報１６およびアクセスチケット１３を保持し、証明データ生成プログラム１７を実行する。ユーザ固有情報１６および証明データ生成プログラム１７の少なくとも一部が耐タンパー装置２０で保護されている。

【００３８】アクセスチケット生成装置１２はアクセス資格認証の特徴情報１４およびユーザの固有情報１６に基づいてアクセスチケット１３を生成し、アクセスチケット１３はネットワークや記憶媒体等を通してユーザに送られ、ユーザの証明データ生成装置１１に保持される。

【００３９】証明データ検証装置１０は認証用データ１８を証明データ生成装置１１に送信する。証明データ生成装置１１はアクセスチケット１３およびユーザ固有情報１６を用いて証明データ１９を生成し、これを証明データ検証装置１０に返信する。証明データ検証装置１０は認証用データに基づいて証明データの正当性を検証する。即ち、証明データが、検証用データとアクセス資格認証の特徴情報とに基づいて生成されたデータであることを検証する。

【００４０】証明データの正当性が検証されれば、ユーザが正当な権利を有することが認証され、サービス提供装置により所望のサービスが提供される。

【００４１】以下、図２を用い、実際のサービスを例にとって本発明を具体的に説明する。

【００４２】本発明の実施例１では、インターネットブラウザ（Ｎｅｔｓｃａｐｅ　Ｎａｖｉｇａｔｏｒ－米国ネットスケープ・コミュニケーションズ社の商標－等）に、証明データ検証ルーチン１５と復号プログラム３５とを一体化してプラグイン（Ｐｌｕｇ－Ｉｎ）モジュールとして組み込んだ例について述べる。ここで、プラグイン・モジュールとはインターネットブラウザの機能を拡張するソフトウエアプログラムを指し、これにより、ユーザに新しいデータタイプの利用をサポートすることができる。インターネットブラウザがサポートしていないデータタイプの情報をサーバから受け取ると、インターネットブラウザは、そのデータタイプに関連付けられているプラグインを探してロードし、起動する。これにより、ユーザの既存のシステムを変更することなく、シームレスに新しいデータタイプのサポートを可能にするものである。

【００４３】本実施例の場合の新しいデータタイプとは暗号化されたコンテンツ３４を指し、インターネットブラウザが暗号化されたコンテンツ３４をサーバから受け取ると、インターネットブラウザは暗号化されたコンテンツ３４のデータタイプを見て、そのデータタイプに関連付けられているプラグイン３８を探してロードし、起動する。起動されたプラグインは、検証ルーチン１５を起動し、証明用プログラム３２に認証用データを送り、返ってきた証明データを用いて検証を行う。検証ルーチン１５により検証が成功した場合には復号プログラム３５によって、暗号化されたコンテンツ３４が復号されてユーザに提供される。復号されたコンテンツは、ハイパードキュメント、画像、動画、音楽などの情報やダウンロードしたプログラムなどである。

【００４４】証明データ生成装置は、証明用プログラム３２とトークン３３とで構成される。認証用プログラム３２はアクセスチケット１３と認証データ生成プログラムＡ３６を含むソフトウエアプログラムであり、ユーザのパーソナルコンピュータ（ＰＣ）上で動作する。トークン３３は認証データ生成プログラムＢ３７とユーザ固有情報１６とを含み、プローブによる内部状態の窃盗への防御力を有するハードウエア（以下、耐タンパハードウエアと呼ぶ）により構成することが望ましい。なぜならば、ユーザ個有情報は、パスワード認証におけるパスワードに相当するものであり、ユーザの身許を証明する唯一の重要な情報であり、ユーザ固有情報１６を読み出しコピーして配布することができると、正当な権利を持たない者にコンテンツの不正利用を許してしまうことになる。

【００４５】また、ユーザには前記ユーザ固有情報に加え、所定の計算手続きを実行する証明データ生成プログラムＡ、Ｂが与えられる。このプログラムは、プラグイ

ン３８中の検証ルーチン１５と通信を行うためのものであり、ユーザ固有情報１６とアクセスチケット１３が与えられると、認証用データ４２に対して計算を行いユーザの身許を証明する証明データ４５を生成する。この計算の過程でユーザ固有情報１６が用いられるが、上述した理由によりユーザ固有情報１６が外部に漏洩すると問題があるため、ユーザ固有情報を用いる証明データ生成プログラムＢ３７は前記耐タンパハードウエア内に収められる。耐タンパハードウエアとしては、ＩＣカードや樹脂モールド等で保護されたＩＣチップなどが簡便で適用しやすい。しかし、提供するサービスの付加価値が非常に高い場合は、特願平０８－２８４４７５号の「暗号化装置、復号装置、機密データ処理装置、および情報処理装置」で示されるような、高い安全性を有する装置を用いてもよい。

【００４６】証明データ検証ルーチン１５の作用を以下に数例述べる。

【００４７】１．証明データ検証ルーチン１５中には、送信するべきデータ（認証用データ４２）と期待される返信データ（期待値）が埋入されている。証明データ検証ルーチン１５は、前記送信データを取り出してユーザに送信し、ユーザから返信を受け取る。次いで、ユーザからの返信データと前記期待値とを比較して、両者が一致した場合に復号プログラム３５により暗号化されたコンテンツ３４を復号して、ユーザに利用可能な状態でコンテンツを提供する。

【００４８】２．証明データ検証ルーチン１５中には、送信するべきデータと期待される返信データ（期待値）が埋入されている。証明データ検証ルーチン１５は、前記送信データを取り出してユーザに送信し、ユーザから返信を受け取る。次いで、ユーザからの返信データに一方向性関数を施した値を、前記期待値と比較して、両者が一致した場合に復号プログラム３５により暗号化されたコンテンツ３４を復号して、ユーザに利用可能な状態でコンテンツを提供する。

【００４９】上記１，２の作用において、返信データが送信データの所定の暗号化アルゴリズムに従う暗号化の結果であるとした場合には、アクセス資格認証の特徴情報は暗号化鍵となる。また、返信データが送信データの所定の署名アルゴリズムに従うデジタル署名であるとした場合には、アクセス資格認証の特徴情報は署名鍵となる。

【００５０】３．証明データ検証ルーチン１５中には、送信するべきデータが埋入されている。証明データ検証ルーチン１５は、前記送信データを取り出してユーザに送信し、ユーザから返信を受け取る。次いで、前記返信データを復号鍵として、復号プログラム３５により暗号化されたコンテンツ３４を復号して、ユーザに利用可能な状態でコンテンツを提供する。

【００５１】４．証明データ検証ルーチン１５中には、送信するべきデータが埋入されている。証明データ検証ルーチン１５は、前記送信データを取り出して乱数効果を付与した後ユーザに送信し、ユーザから返信を受け取る。次いで、前記返信データから前記乱数効果を取り除いた結果を復号鍵として、復号プログラム３５により暗号化されたコンテンツ３４を復号して、ユーザに利用可能な状態でコンテンツを提供する。

【００５２】５．証明データ検証ルーチン１５は、暗号化されたコンテンツに対応した送信データを受け取る。この場合、送信データは暗号化されたコンテンツの中に埋入されていてもよい。証明データ検証ルーチン１５は、受け取った前記送信データをユーザに送信し、ユーザから返信を受け取る。次いで、前記返信データを復号鍵として、復号プログラム３５により暗号化されたコンテンツ３４を復号して、ユーザに利用可能な状態でコンテンツを提供する。

【００５３】６．証明データ検証ルーチン１５は、暗号化されたコンテンツに対応した送信データを受け取る。この場合、送信データは暗号化されたコンテンツの中に埋入されていてもよい。証明データ検証ルーチン１５は、受け取った前記送信データに乱数効果を付与した後ユーザに送信し、ユーザから返信を受け取る。次いで、前記返信データから前記乱数効果を取り除いた結果を復号鍵として、復号プログラム３５により暗号化されたコンテンツ３４を復号して、ユーザに利用可能な状態でコンテンツを提供する。

【００５４】上記3乃至6の作用において、返信データから正しい復号鍵が得られた場合にかぎって、暗号化されたコンテンツ３４は正しく復号され、ユーザは該コンテンツを利用可能となる。この場合のアクセス資格認証の特徴情報は暗号化された復号鍵を復号するための復号鍵となる。

【００５５】さて、従来の例で述べた実行制御技術では、ユーザ固有情報（ユーザの認証鍵）がアクセス資格認証の特徴情報と同一のものである。従来の証明データ生成ルーチンはアクセス資格認証の特徴情報と証明データ検証ルーチンから送信されたデータとを入力して、返信データを計算する。

【００５６】これに対し本発明の特徴は、ユーザ固有情報１６とアクセス資格認証の特徴情報１４とが互いに独立である点にある。この構成でも、証明データ生成プログラムＡとＢはユーザ固有情報１６と証明データ検証ルーチン１５から送信されたデータ４２に加えて、アクセスチケット１３を入力として返信データ（証明データ）４５を計算する。この構成は以下の性質を持つ。

【００５７】１．アクセスチケット１３は特定のユーザ固有情報１６とアクセス資格認証の特徴情報１４とに基づいて計算されるデータである。

２．ユーザ固有情報１６を知らずにアクセスチケット１３から、アクセス資格認証の特徴情報１４を計算するこ

とは少なくとも計算量的に不可能である。

３．証明データ生成プログラムＡとＢは、ユーザ固有情報１６とアクセスチケット１３とが正しい組み合わせの場合、即ち、ユーザ固有情報１６とアクセスチケット１３との正しい組み合わせが入力された場合に限って、正しい返信データを計算する。

【００５８】以上により、ユーザはあらかじめユーザ固有情報１６を所持し、コンテンツ作成者はユーザが所持するユーザ固有情報１６とは独立にコンテンツを暗号化し、アクセスチケット１３をユーザ固有情報１６とアクセス資格認証の特徴情報とに応じて作成することで、正当な権利を有するユーザにのみユーザ固有情報１６とは独立に暗号化されたコンテンツの利用を享受することができる。

【００５９】また、ユーザ固有情報１６を二つの固有情報からなるものとし、アクセスチケット１３の作成に際して用いる固有情報と、ユーザが通信プログラムにおいて用いる固有情報とを区別して用いることもできる。最も典型的な例は、ユーザ固有情報１６を公開鍵ペアとし、公開鍵を公開固有情報としてアクセスチケット作成に用い、秘密鍵をユーザ個人の秘密固有情報としてトークン３３内に封入しておく方法である。この場合はアクセスチケット１３をアクセス資格認証の特徴情報１４と前記公開鍵ペアの公開鍵から計算できるようにすることにより、秘密鍵であるユーザ固有情報１６を秘密に保ったままアクセスチケット１３を計算することが可能となる。

【００６０】次により具体的な構成について実施例に則して説明する。図２において、インターネットブラウザ３１とプラグイン３８と証明用プログラム３２は、ユーザの用いる計算機３０（ＰＣあるいはワークステーション）上のソフトウエアプログラムとして実現することができる。トークン３３についても同様にソフトウエアプログラムとして実現してもよいが、ユーザを識別するための固有情報（ユーザ固有情報）の安全性を高めるために、該計算機３０に接続される耐タンパ特性を有するトークン３３（ＩＣカード、ＰＣカード、ボード等）を併用するのが望ましい。この際、ＩＣカードのような携帯性を有するハードウエアを用いれば、ユーザが複数のＰＣあるいはワークステーション上で作業する場合に便利である。

【００６１】インターネットブラウザ３１で利用する暗号化されたコンテンツ３４は、ネットワークやＣＤ－ＲＯＭ、ＤＶＤ、フロッピーディスク等の記憶媒体を用いてユーザに供給される。

【００６２】ユーザがインターネットブラウザから暗号化されたコンテンツの利用を要求すると、インターネットブラウザは暗号化されたコンテンツのデータタイプを見て、そのデータタイプに関連付けられているプラグインを探してロードし、起動する。

【００６３】プラグインが起動すると、該プラグイン中の検証プログラムが起動し、証明用プログラム３２と通信してユーザ認証を行い、通信が正しく終了した場合に限って、該コンテンツの復号を実行する。

【００６４】ユーザが暗号化されたコンテンツ３４を利用するためには、ユーザ本人宛に発行されたアクセスチケット（証明用補助情報）を取得する必要がある。ユーザは前記ＰＣあるいはワークステーション上にインストールされた証明用プログラム３２に、取得したアクセスチケットを登録するとともに、例えばユーザ固有情報がＩＣカードに封入されている場合には、ＩＣカードを前記ＰＣあるいはワークステーションに装着する。

【００６５】証明データ生成プログラムＡは、証明データ生成プログラムＢと協調して、ユーザ固有情報１６とアクセスチケット１３とに基づいて計算を行い、その計算に基づいてプラグイン中の検証プログラム１５と通信を行う。

【００６６】通信の結果、検証プログラム１５による認証が成功するのは、ユーザ固有情報と、アクセスチケットと、暗号化されたコンテンツとの３つが正しく対応している場合に限る。ユーザ固有情報あるいはアクセスチケットの一方が欠けていた場合には認証は成功しない。

【００６７】アクセスチケットは特定のユーザ宛に発行される。即ち、アクセスチケットの生成に際して、特定のユーザのユーザ固有情報が使用される。アクセスチケット生成時に使用されるユーザ固有情報と、証明データ生成プログラムによって使用される前記ユーザ固有情報とが一致していない場合、やはり、認証は成功しない。

【００６８】また、アクセスチケットは、特定のアクセス資格認証の特徴情報に基づいて生成され、検証プログラム１５はこのアクセス資格認証の特徴情報を認証するように構成される。従って、アクセスチケットの生成のもととなった特徴情報と、検証プログラム１５が認証しようとする特徴情報とが互いに対応していなかった場合にも、認証は成功しない。

【００６９】アクセスチケットは、それ自身十分な安全性を備えていることから、ネットワークを介して配送することができる。アクセスチケットの安全性とは、以下の二つの性質である。

【００７０】１．アクセスチケットは記名式であり、アクセスチケットが発行されたユーザ本人（正確には、アクセスチケット生成時に用いられたユーザ固有情報の保持者）だけが該アクセスチケットを用いて証明データ生成装置を正しく作動させることができる。従って、悪意の第三者がネットワークを盗聴し、他のユーザのアクセスチケットを不正に手に入れたとしても、この第三者がアクセスチケットの発行先である正規のユーザ固有情報を手に入れない限り、このアクセスチケットを利用することは不可能である。

【００７１】２．アクセスチケットはさらに厳密な安全

性を保持している。即ち、悪意の第三者が任意の個数のアクセスチケットを集めて、いかなる解析を行ったとしても、得られた情報をもとに別のアクセスチケットを偽造したり、証明データ生成装置の動作を模倣して認証を成立させるような装置を構成することは不可能である。

【００７２】実施例１では、アクセスチケットｔは次の式１に基づいて生成されるデータである。

【００７３】

【数１】

（１）　ｔ＝Ｄ－ｅ＋ωϕ（ｎ）

上式中の記号はすべて整数であり、以下を表す。ｎはＲＳＡ（Ｒｉｖｅｓｔ－Ｓｈａｍｉｒ－Ａｄｅｌｍａｎ）法数、即ち十分大きな二つの素数ｐ、ｑの積である（ｎ＝ｐｑ）。ϕ（ｎ）はｎのオイラー数、即ち、ｐ－１とｑ－１の積である（ϕ（ｎ）＝（ｐ－１）（ｑ－１））。ｅはユーザ固有情報を表し、ユーザ毎に異なる数で、ユーザを識別するために用いる。Ｄはアクセスチケット秘密鍵すなわちアクセス資格認証の特徴情報を表し、法数ｎのもとでのＲＳＡ秘密鍵であり、式２を満たす。

【００７４】

【数２】（２）　ｇｃｄ（Ｄ，ϕ（ｎ））＝１

ここで、ｇｃｄ（ｘ，ｙ）は二数ｘ、ｙの最大公約数を表す。式（２）によって表現される性質は、式３を満たす数Ｅが存在することを保証する。

【００７５】

【数３】（３）　ＥＤ　ｍｏｄ　ϕ（ｎ）＝１

Ｅをアクセスチケット公開鍵と呼ぶ。

【００７６】ωは、ｎおよびｅに依存して定まる数であり、ｎあるいはｅのいずれか一方が異なる場合、その値が容易に一致しない（衝突しない）ように定める。ωの定め方の一例として、一方向性ハッシュ関数ｈを利用して、式４のようにωを定める方法もある。

【００７７】

【数４】（４）　ω＝ｈ（ｎ｜ｅ）

ただし、記号｜はビット列の結合を表す。

【００７８】一方向性ハッシュ関数とは、ｈ（ｘ）＝ｈ（ｙ）を満たす相異なるｘ、ｙを算出することが著しく困難であるという性質を持つ関数である。一方向性ハッシュ関数の例として、ＲＳＡ　Ｄａｔａ　Ｓｅｃｕｒｉｔｙ　Ｉｎｃ．によるＭＤ２、ＭＤ４、ＭＤ５、および米国連邦政府による規格ＳＨＳ（Ｓｅｃｕｒｅ　Ｈａｓｈ　Ｓｔａｎｄａｒｄ）が知られている。

【００７９】上記の説明中に現れた数において、ｔ、Ｅおよびｎは公開可能であり、残りのＤ、ｅ、ω、ｐ、ｑおよびϕ（ｎ）はチケットを作成する権利を有する者以外には秘密である必要がある。

【００８０】図３に、ユーザが用いる計算機（ＰＣあるいはワークステーション）の概略図を示す。図３においては、ユーザが用いる計算機３０に、カードリーダ３９が接続されており、ユーザはカードリーダ３９にトークン３３を挿入して利用する。インターネットブラウザ３１、プラグイン、証明用プログラムは、計算機３０上のソフトウエアプログラムとして実現されている。また、アクセスチケットも計算機３０の記憶領域に記憶されている。今、利用しようとしているコンテンツは、ヨットの絵の画像であり、正当なトークンと正当なアクセスチケットを持つユーザが、暗号化されたコンテンツをインターネットブラウザ３１に読み込ませると、図３に示すようにプラグインによってインターネットブラウザ３１上に、ヨットの絵の画像が表示される。

【００８１】図４を参照してさらに実施例１について詳細に説明する。図４は、本発明の実施例１の構成例を具体的に示すものである。図２と対比させると検証ルーチン１５に対応するものは、アクセスチケット公開鍵記憶部５１、認証データ記憶部５２、乱数発生部５３、乱数記憶部５４、送信データ（チャレンジ）計算部５５、データ分離部５６、証明データ受信部５７、乱数効果除去部５８、および検証部５９とで構成され、復号プログラム３５は、復号／表示部６１に対応する。この例では検証ルーチンと復号プログラムとを分けて構成してあるが、必要に応じて復号プログラムを検証ルーチンに併合させてもよい。また、証明用プログラム３２は、認証用データ受信部７１、アクセスチケット記憶部７２、第１演算部７３および証明データ生成部７６とで構成され、トークン３３はユーザ固有情報記憶部７４および第２演算部７５とで構成される。

【００８２】次に、動作について説明する。以下の説明における変数は、すべて整数である。

【００８３】［ステップ１］：ユーザがインターネットブラウザから暗号化されたコンテンツの利用を要求すると、インターネットブラウザは暗号化されたコンテンツのデータタイプを見て、そのデータタイプに関連付けられているプラグインを探してロードし、起動する。対応するプラグインが起動すると、プラグイン中の検証ルーチン１５が立ち上がる。この場合のコンテンツとはユーザがインターネットブラウザを通して利用するようなものを指し、例えばホームページの表示情報（画像、動画、ハイパードキュメントなど）であったり、Ｊａｖａアプレットのようなプログラムであったりする。

【００８４】［ステップ２］：プラグインの検証ルーチン１５は、データ分離部において暗号化されたコンテンツからアクセスチケット公開鍵（Ｅ，ｎ）と認証データK^Eを取り出し、それぞれアクセスチケット公開鍵記憶部５１と認証データ記憶部５２に格納する。ここでは、該アクセスチケット公開鍵と該認証データは、暗号化されたコンテンツに付随して配布されているものとして説明した。このように該アクセスチケット公開鍵と該認証データは、暗号化されたコンテンツに付随していてもよいしネットワークを通して入手できるようにしてもよい

が、安全性を考えると暗号化されたコンテンツに付随しているのが望ましく、さらに、該認証データは、ユーザにはわからないように埋め込まれていることが望ましい。例えば、該認証データは、暗号化してコンテンツの中に埋め込んでおき、取り出したあと、プラグインに持たせた復号鍵で復号するなどの方法を取ればよい。

【００８５】［ステップ３］：次に、検証ルーチン１５は、乱数生成部５３で乱数ｒを生成し乱数記憶部５４に格納し、アクセスチケット公開鍵（Ｅ，ｎ）と認証データK^Eおよび乱数ｒを用いて送信データ（チャレンジ）Ｃを式５に従って計算する。

【００８６】

【数５】（５）　$C=r^E K^E \mod n$

チャレンジＣとアクセスチケット公開鍵法数（ＲＳＡ法数）ｎは、証明データ生成側に送信される。Ｃの値には乱数ｒが含まれているため、通信の度に異なる値となり、リプレイアタックを防止する効果を持つ。

【００８７】［ステップ４］：証明用プログラムでは、検証ルーチンから送られたチャレンジＣとＲＳＡ法数ｎとを認証用データ受信部で受信し、証明データ（レスポンス）Ｒを以下のようにして生成する。まず、第１演算部ではアクセスチケット記憶部７２から、ＲＳＡ法数ｎをキーにして対応するアクセスチケットｔを取得し、ＲＳＡ法数ｎのもとで、式６を実行し中間情報Ｒ’を得る。

【００８８】

【数６】（６）　$R'=C^t \mod n$

［ステップ５］：第２演算部７５は、ユーザ固有情報記憶部７４に記憶されているユーザ固有情報ｅを取得し、式７を実行し差分情報Ｓを得る。

【００８９】

【数７】（７）　$S=C^e \mod n$

［ステップ６］：そして、証明データ生成部７６は第１および第２演算部７３、７５から中間情報Ｒ’および差分情報Ｓを得て、式８の計算を行い証明データＲを得る。

【００９０】

【数８】（８）　$R=R'S \mod n$

証明データＲは、検証ルーチンに送信される。

【００９１】［ステップ７］：検証ルーチン１５の乱数効果除去部５８は、証明データ受信部５７で受信した証明データＲを取得し、乱数記憶部５４に記憶されている乱数ｒとにより、式９の計算を行いＫ’を得る。

【００９２】

【数９】（９）　$K'=Rr^{-1} \mod n$

［ステップ８］：検証部５９では、前記乱数効果除去部５８で計算したＫ’がアクセス資格認証の特徴情報であるＤに基づいて生成されていることを検証する。Ｋ’が正しくアクセス資格認証の特徴情報であるＤに基づいて生成されている場合には、Ｋ’＝Ｋが成り立つはずである。この式が成り立つかどうかは、このＫ’を用いて暗号化されたデータを復号してみて、正しく復号されるかどうかを判定する方法や、Ｋに冗長性をもたせ、その部分に特定の値を持たせておき、Ｋ’がその特定の値を持っているかどうかで判定する方法などがある。後者の方法には、国際規格ＩＳＯ９７９６などの方法を用いることができる。ここでは、後者の方法を用いて、検証することを前提に説明を続ける。

【００９３】［ステップ９］：検証部５９での検証が正しいと判定されると、検証ルーチンは復号／表示部６１へ復号鍵Ｋ’を渡す。

【００９４】［ステップ１０］：復号／表示部６１は、検証部５９から復号鍵Ｋ’を受け取り、データ分離部５６で分離した暗号化されたコンテンツを復号して表示する。復号されたコンテンツをインターネットブラウザへ渡して、インターネットブラウザで表示する方法も可能であるが、復号された情報がインターネットブラウザによりコピーされる可能性があるため、安全性の面からは、インターネットブラウザが指定した領域にプラグインが直接表示するほうが望ましい。

【００９５】このようにして、正当な権利を有するユーザはインターネットブラウザを用いて暗号化されたコンテンツを利用することができる。このとき、復号されたコンテンツは一時的にしかメモリ上に存在せず、ユーザの利用が終わると消滅するようにすることで、復号されたコンテンツの不正利用を防ぐことができる。

【００９６】本実施例では、暗号化されたコンテンツは、アクセスチケット公開鍵（Ｅ，ｎ）と認証データK^Eとを付随して配布されるものとして説明した。この暗号化されたコンテンツの構成例を図５に示す。図５に示すように、暗号化されたコンテンツは、アクセスチケット公開鍵（Ｅ，ｎ）と、認証データK^Eと、暗号化されたコンテンツ本体とから構成される。検証ルーチンのデータ分離部は、これらを読み込んで、各部分に分離する。

【００９７】コンテンツ本体は鍵Ｋで暗号化されており、認証データK^Eを用いて正しく検証が終了すると、乱数効果除去部を通して鍵Ｋを復元することができ、この鍵Ｋを用いてコンテンツ本体を復号することが可能になる。

【００９８】安全性をより高めるためには、認証データK^Eがユーザには容易に分離できないように埋め込まれていることが望ましい。この実現の一方法を、図６に示す。図６では、図５と同様に、暗号化されたコンテンツは、アクセスチケット公開鍵（Ｅ，ｎ）と認証データK^Eと暗号化されたコンテンツ本体とから構成されるが、コンテンツ本体だけでなく、認証データK^Eもさらに暗号化されている。図６では、認証データK^Eは鍵K_pにより暗号化されているものとして示した。

【００９９】検証ルーチンのデータ分離部は、この暗号

鍵鍵K_Pに対応する復号鍵K_Pを保持しており（共通鍵暗号を用いる例）、入力されたコンテンツ全体から、アクセスチケット公開鍵（Ｅ，ｎ）と、暗号化された認証データK^Eと、暗号化されたコンテンツ本体とを分離し、保持している復号鍵K_Pを用いて暗号化された認証データを復号して、認証データK^Eを取り出す。その後、この認証データK^Eを用いて検証を行い、正しく検証が終了すると、乱数効果除去部を通して鍵Ｋを復元することができ、この鍵Ｋを用いてコンテンツ本体を復号することが可能になる。

【０１００】ここでは、コンテンツ本体や認証データを暗号化するのに、共通鍵暗号方式を用いた例を示したため、鍵Ｋや鍵K_Pは暗号化と復号化とで同じ鍵を用いる例として示したが、この部分をＲＳＡなどの公開鍵暗号方式を用いることも可能である。

【０１０１】また、コンテンツの最も単純な構成例を図７に示す。この例では、コンテンツはコンテンツ本体のみから構成されており、コンテンツ本体も暗号化などの処理が行われていない。しかし、このコンテンツを利用してサービスを提供できるのは特定のプラグインだけであるという状況にある。プラグイン中の検証ルーチンでは、前述したのと同様な処理を行い、検証部における判定の結果、正当であると判断された場合にのみ、プラグインはこのコンテンツを用いてサービスを提供する。

【０１０２】以下では、実施例１において説明した検証ルーチンの検証部における処理の構成例を図８～図１１を用いて数例述べる。図８～図１１では、主に検証ルーチンの中の検証部５９についての構成を示している。ここでは各構成例の違いを明確にするために、検証部５９の中に比較部５９１や期待値記憶部５９２があるような構成として示したが、これに限らず期待値記憶部５９２などは検証部５９の外側に構成しても構わない。

【０１０３】（１）検証部５９の構成例の１を図８に示す。この構成例では、検証部５９は、期待値記憶部５９２と、比較部５９１とを有し、期待値記憶部５９２には証明データとして期待している期待値Ａを記憶している。検証部５９への入力には、証明プログラムから受信した証明データ、あるいは認証データ生成時に乱数効果を付与した場合には受信した証明データから乱数効果を除去した証明データが入力される。この入力された証明データＡ’と、期待値記憶部５９２に記憶している期待値Ａとを比較部５９１で比較する。比較の結果、正当と判定された時には、表示部（復号／表示部６１）に正当の判定を渡し、表示部はデータを表示する。

【０１０４】この構成の場合、期待値記憶部５９２に記憶している期待値Ａがプログラム解析などによって窃取されることは、困難ではあっても不可能ではない。期待値Ａが窃取されると、乱数効果を付与する際の乱数が予想可能であると、証明プログラムの動作を模倣する装置を構成することが可能となり、なりすましによる不正アクセスが可能となる。このようなことを防ぐためには、逆方向への変換が困難な性質を持つ一方向性関数ｈ（）を用いて、期待値記憶部５９２に記憶する期待値として、Ａに一方向性関数ｈ（）を施して得られるデータｈ（Ａ）を記憶しておき、検証部５９１に入力された証明データＡ’に対して、一方向性関数ｈ（）を施した結果のデータｈ（Ａ’）との比較を行うようにすればよい。このように構成することで、万一、期待値記憶部５９２に記憶している期待値ｈ（Ａ）が窃取されたとしても、ｈ（Ａ）からＡを計算することは著しく困難であるので、上記のようなりすましを防ぐことができる。

【０１０５】（２）検証部５９の構成例の２を図９に示す。この構成例では、検証部５９は、期待値記憶部５９２と、比較部５９１と復号鍵記憶部５９３とを有し、期待値記憶部５９２には証明データとして期待している期待値Ａを記憶している。検証部５９への入力には、証明プログラムから受信した証明データ、あるいは認証データ生成時に乱数効果を付与した場合には受信した証明データから乱数効果を除去した証明データが入力される。この入力された証明データＡ’と、期待値記憶部５９２に記憶している期待値Ａとを比較部で比較する。比較の結果、正当と判定された時には、復号鍵記憶部５９３から復号／表示部６１に復号鍵Ｋを渡し、復号／表示部６１はこの復号鍵Ｋを用いて暗号化データを復号し、データを表示する。

【０１０６】構成例１と同様に、一方向性関数ｈ（）を用いることも可能である。

【０１０７】（３）検証部５９の構成例の３を図１０に示す。この構成例では、構成例１と同様に検証部５９は、期待値記憶部５９２と、比較部５９１とを有するが、期待値記憶部５９２には期待値として復号鍵Ｋを記憶している。構成例１と同様に、入力された証明データＫ’と、期待値記憶部５９２に記憶している期待値Ｋとを比較部５９１で比較する。比較の結果、正当と判定された時には、復号／表示部６１に復号鍵Ｋ’を渡し、復号／表示部６１はこの復号鍵Ｋを用いて暗号化データを復号し、データを表示する。

【０１０８】（４）検証部５９の構成例の４を図１１に示す。この構成例では、検証部５９は、冗長性検査部５９４を有している。検証部５９への入力には、証明プログラムから受信した証明データ、あるいは認証データ生成時に乱数効果を付与した場合には受信した証明データから乱数効果を除去した証明データが入力される。この入力された証明データＫ’を冗長性検査部５９４で検査する。この方法は、前述したように予めＫに冗長性を持たせておき、Ｋ’がその冗長性を持っているかどうかを検査するものである。例えば、国際規格ＩＳＯ９７９６などの方法を用いることができる。冗長性検査部５９４で冗長性の検査に合格すると、冗長性検査部５９４は復号／表示部６１に復号鍵Ｋ’を渡し、復号／表示部６１

はこの復号鍵Ｋを用いて暗号化データを復号し、データを表示する。

【０１０９】［実施例２］つぎに本発明の実施例２について説明する。本発明の実施例１では、証明データ生成装置１１によって生成された証明データが検証用データとアクセス資格認証の特徴情報とに基づいて生成されたデータであることを、証明データ検証装置１０の検証ルーチン１５が検証し、証明データの正当性が検証されたときに限って、サービスが提供されるサービス提供装置について、インターネットブラウザに、証明データ検証ルーチン１５と復号プログラム３５とを一体化してプラグイン・モジュールとして組み込んだ例について述べた。実施例１では、検証ルーチン１５が受信した証明データから乱数効果を除去した結果が、復号／表示部により復号するための復号鍵になり、その復号鍵が正当なものであるかどうかを判定して、正当なものであるときのみその復号鍵を用いて、暗号化データを復号してサービスを提供するものであった。

【０１１０】しかし、実施例１のように、証明データから乱数効果を除去した結果を復号鍵として用いる例では、必ずしもその復号鍵の正当性を判定する必要はない。証明データから乱数効果を除去した結果をそのまま復号鍵として用いて、暗号化データを復号することにより、正当な復号鍵である場合には、正しく復号が成功してサービスを提供することが可能になり、正当な復号鍵でない場合には、復号は成功せずに、サービスを提供することができないという結果になるだけである。

【０１１１】実施例２では、このように検証部のない例について説明する。以下、実施例２では、検証ルーチンという言葉は用いるが、この検証ルーチンには検証部は存在しない。つまり、検証が成功したかどうかを判定する部分は存在しない。暗号化されたコンテンツからアクセスチケット公開鍵（Ｅ，ｎ）と認証データK^Eを取り出し、それらを用いて認証用データを生成して証明プログラムに送信し、証明プログラムから返送された証明データから乱数効果を除去した結果を、復号鍵として復号／表示部に渡す処理を行うものである。

【０１１２】図１２は、実施例２の構成例を示したものである。図１２は、図４から検証部５９をなくした構成であり、それ以外は図４と同じ構成である。

【０１１３】動作についても、実施例１で説明したのとほとんど同じであり、［ステップ１］～［ステップ７］は同じ処理を行う。以下、［ステップ８］以降について説明する。

【０１１４】［ステップ８］：ステップ７により検証ルーチンの処理は終了し、検証ルーチンは、前記乱数効果除去部５８で計算したＫ’を復号鍵として復号／表示部６１へ渡す。

【０１１５】［ステップ９］：復号／表示部６１は、検証ルーチンの乱数効果除去部５８から復号鍵Ｋ’を受け取り、データ分離部５６で分離した暗号化されたコンテンツを復号して表示する。証明プログラムにおいて、正当なトークンを持つユーザが正当なアクセスチケットを用いて証明データを生成したときのみ、復号鍵Ｋ’は正しい復号鍵になり、暗号化されたコンテンツが正しく復号されて表示される。トークンまたはアクセスチケットが正当でない時には、復号鍵Ｋ’は正しい復号鍵とはなり得ず、暗号化されたコンテンツは正しく復号されないため、正しい表示がされないことになる。

【０１１６】［実施例３］つぎに本発明の実施例３について説明する。図１３は本発明の実施例３の構成を示している。この実施例３は証明データ検証側で上記とは異なるプロトコルを用いた例であり、実施例１の図８（ｂ）で示した検証部の構成要素を、検証部の外に出した構成に近いものである。図４と対応するものは同じ番号で示してある。図１３において、８１は復号鍵記憶部を表し、コンテンツを復号するための復号鍵Ｋを検証ルーチンが予め保持している。

【０１１７】暗号化されたコンテンツの構成は、暗号化されたコンテンツ本体と、アクセスチケット公開鍵とで構成されており、認証データを含む必要はない。

【０１１８】次に、動作について説明する。以下の説明における変数は、すべて整数である。

【０１１９】［ステップ１］：ユーザがインターネットブラウザから暗号化されたコンテンツの利用を要求すると、インターネットブラウザは暗号化されたコンテンツのデータタイプを見て、そのデータタイプに関連付けられているプラグインを探してロードし、起動する。対応するプラグインが起動すると、プラグイン中の検証ルーチン１５が立ち上がる。この場合のコンテンツとはユーザがインターネットブラウザを通して利用するようなものを指し、例えばホームページの表示情報（画像、動画、ハイパードキュメントなど）であったり、Ｊａｖａアプレットのようなプログラムであったりする。

【０１２０】［ステップ２］：プラグインの検証ルーチン１５は、データ分離部において暗号化されたコンテンツからアクセスチケット公開鍵（Ｅ，ｎ）を取り出し、アクセスチケット公開鍵記憶部５１に格納する。

【０１２１】［ステップ３］：次に、検証ルーチン１５は、乱数生成部５３で乱数ｒを生成し乱数記憶部５４に格納し、乱数ｒを送信データ（チャレンジ）Ｃとして、チャレンジＣとアクセスチケット公開鍵法数（ＲＳＡ法数）ｎとを、証明データ生成側に送信する。この場合、証明用プログラムが返す証明データは、チャレンジＣを法数ｎのもとで、ＲＳＡ暗号を用いて暗号化したものになるはずである。

【０１２２】［ステップ４］：証明用プログラムでは、検証ルーチンから送られたチャレンジＣとＲＳＡ法数ｎとを認証用データ受信部で受信し、証明データ（レスポンス）Ｒを以下のようにして生成する。まず、第１演算

部ではアクセスチケット記憶部７２から、ＲＳＡ法数ｎをキーにして対応するアクセスチケットｔを取得し、ＲＳＡ法数ｎのもとで、式６を実行し中間情報Ｒ’を得る。

【０１２３】［ステップ５］：第２演算部７５は、ユーザ固有情報記憶部７４に記憶されているユーザ固有情報ｅを取得し、式７を実行し差分情報Ｓを得る。

【０１２４】［ステップ６］：そして、証明データ生成部７６は第１および第２演算部７５から中間情報Ｒ’および差分情報Ｓを得て、式８の計算を行い証明データＲを得る。証明データＲは、検証側に送信される。

【０１２５】［ステップ７］：検証ルーチン１５の検証部５９は、受信した証明データＲを取得し、式１０の計算を行い乱数記憶部５４に記憶されている乱数ｒと計算結果ｒ’とを比較することにより検証を行う。

【０１２６】

【数１０】（１０）　　$r' = R^{E} \mod n$

乱数ｒと計算結果ｒ’とが等しいとき検証は成功したとみなされ、検証ルーチン１５は復号鍵Ｋを復号／表示部へ渡す。

【０１２７】［ステップ８］：復号／表示部６１は、検証部５９から復号鍵Ｋを受け取り、データ分離部５６で分離した暗号化されたコンテンツを復号して表示する。復号されたコンテンツをインターネットブラウザへ渡して、インターネットブラウザで表示する方法も可能であるが、復号された情報がインターネットブラウザによりコピーされる可能性があるため、安全性の面からは、インターネットブラウザが指定した領域にプラグインが直接表示するほうが望ましい。

【０１２８】このように、検証ルーチンではユーザが正当な権利を有することのみを検証し、検証が成功した場合に、予め登録されていた復号鍵で暗号化されたコンテンツを復号するようにしてもよい。

【０１２９】上記第１ないし実施例３で検証ルーチンの部分をソフトウエアプログラムで構成する例を示したが、その場合、コンテンツの復号鍵Ｋは秘密にしておかなければならない。なぜなら、Ｋが漏洩してしまうと暗号化されたコンテンツは誰でも復号できることになってしまい、コンテンツの不正利用を許してしまうこととなる。従って、検証ルーチンは何らかの方法で内部データを保護する必要がある。そのような方法として、プログラムをマシン語にコード化する際に内部データやプログラム手順が解析し難くなるように難読化する方法がある。これらの技術は、村上隆徳ら「プログラムコードの難読化について」，電子情報通信学会技術研究報告（ＩＥＩＣＥ　Ｔｅｃｈｎｉｃａｌ　Ｒｅｐｏｒｔ）情報セキュリティ，ＩＳＥＣ９５－２５（１９９５）等で紹介されている。また、ソフトウエア的手法以外に、検証ルーチンと復号プログラムとを１つのハードウエアで構成する方法を用いてもよい。その場合は、専用のハードウエアやＰＣカードおよびＩＣカード等で構成することができる。また、検証ルーチン、証明データ生成部および復号／表示部すべてを１つのハードウエアで構成することも可能である。

【０１３０】［実施例４］つぎに本発明の実施例４について説明する。本実施例では、利用制御情報を用いた構成例について説明する。利用制御情報は、証明データの生成を制御するための制御情報であり、またサービスを提供する条件を記述する制御情報であり、アクセスチケットとともに配布される。制御情報は、例えば、サービスを提供する期限、料金額、回数、時間などを記述することができ、証明データを生成するときに、これらの条件をチェックして、条件に合致しないときには証明データの生成を行わないようにして、サービスの提供をストップすることができる。これ以外にも制御情報には、役職、性別、年齢などのようなユーザの属性を記述しておいて、トークン中に保持されているユーザの属性と比較して、証明データの生成を制御することも可能である。

【０１３１】以下では、制御情報として利用期限を用いたときの説明と、料金額を用いたときの説明を簡単に述べる。

【０１３２】本実施例では、アクセスチケットｔは次の式１１に基づいて生成されるデータである。

【０１３３】

【数１１】

（１１）　　$t = D - F(n, e, L)$

三変数関数Ｆ（ｘ，ｙ，ｚ）は関数値が衝突しにくい三変数関数であり、例えば前述の一方向性ハッシュ関数ｈを利用して式１３のように定めることができる。

【０１３４】

【数１２】

（１２）　　$F(x, y, z) = h(x \mid y \mid z)$

上式中の記号はすべて整数であり、実施例１と同様に、ｎはＲＳＡ法数、Ｄはアクセスチケット秘密鍵、ｅはユーザ固有情報を表す。Ｌは利用制御情報であり、関数Ｆ（）は一方向性関数である。

【０１３５】図１４を参照してさらに本実施例について詳細に説明する。図１４は、本発明の実施例４の構成例を具体的に示すものである。図１４の左半分、つまりプラグインおよび検証ルーチン側は、実施例１の図４と同じである。

【０１３６】証明用プログラム３２は、認証用データ受信部７１、アクセスチケット記憶部７２、第１演算部７３および証明データ生成部７６とで構成され、トークン３３はユーザ固有情報記憶部７４、第２演算部７５および利用制御情報判定部７７とで構成される。

【０１３７】アクセスチケット記憶部７２は、ＲＳＡ法数ｎと、アクセスチケットｔに加えて、利用制御情報Ｌ

とを組にして記憶している。利用制御情報判定部７７は、アクセスチケット記憶部７２から渡された利用制御情報Ｌの条件を判定し、判定の結果正しいと判定したときのみ、利用制御情報Ｌを第２演算部７５に渡す。第２演算部７５では、利用制御情報判定部７７から利用制御情報Ｌを渡されたときのみ、式１３に基づいて差分情報Ｓを計算し、証明データ生成部７６に送る。

【０１３８】

【数１３】

（１３）　$S = C^{F(n,e,L)} \mod n$

以下では、利用制御情報として利用期限を用いたときについて説明する。利用制御情報として利用期限を持つときには、利用制御情報Ｌの値は、例えば１９９７１２３１２４００のような値である。この場合、この値は利用期限が１９９７年１２月３１日２４：００までということを表している。このような数字ではなく、ある日時からの相対的な秒数で表すなどにしてもかまわない。

【０１３９】トークン中の利用制御情報判定部７７は、時計を持ち、アクセスチケット記憶部７２から渡された利用制御情報Ｌと現在の時刻とを比較する。そして比較の結果、利用制御情報Ｌの値が現在の時刻より後である場合には、正しいと判定し、利用制御情報Ｌを第２演算部７５に渡す。第２演算部７５では、利用制御情報判定部７７から利用制御情報Ｌを渡されたときのみ、式１３に基づいて差分情報Ｓを計算し、証明データ生成部７６に送る。

【０１４０】以降、実施例１と同様に、証明データ生成部７６で式８を用いて証明データＲを計算し、検証ルーチン１５の乱数効果除去部５８では、証明データ受信部５７で受信した証明データＲを取得し、乱数記憶部５４に記憶されている乱数ｒとにより、式９の計算を行いＫ’を得る。

【０１４１】正しいアクセスチケットｔと、正しいユーザ固有情報ｅと、正しい利用制御情報Ｌとを用いて計算がなされたときに限って、Ｋ’＝Ｋが成り立ち、検証ルーチン１５の検証部により正しいとの判定が下されて、サービスが提供される。利用制御情報Ｌの利用期限がきれているアクセスチケットを使おうとして、何者かが、アクセスチケット記憶部７２に記憶されている利用制御情報Ｌを改竄したとしても、アクセスチケットｔを改竄することはできないため、証明データ生成部７６で式８を用いて生成された証明データＲは正しい値にはなり得ず、不当にサービスの提供を受けることはできない。

【０１４２】利用制御情報Ｌがサービスの利用額であるときには、例えば利用制御情報Ｌの値として、１回１００円の意味で、１００という数字が与えられている。

【０１４３】トークンは、例えばプリペイドの残高情報を記憶するプリペイド残高記憶部を有し、トークン中の利用制御情報判定部７７は、利用制御情報Ｌとプリペイド残高とを比較して、プリペイド残高の方が大きいときに、正しいと判定し、プリペイド残高から利用制御情報Ｌ分に相当する値を減額して、利用制御情報Ｌを第２演算部７５に渡す。以下の処理は同様である。

【０１４４】また、プリペイド残高記憶部のかわりに、利用履歴記憶部を有し、トークン中の利用制御情報判定部７７は、利用制御情報Ｌの値を時刻などの情報とともに利用履歴記憶部に記録して、利用制御情報Ｌを第２演算部７５に渡すようにしてもよい。この場合には、時々利用履歴記憶部に記憶されている利用履歴を回収して、相当する金額を支払うなどの処理を行う。

【０１４５】このように、ここで示した例以外でも、利用制御情報判定部７７により利用制御情報Ｌをチェックした後で利用制御情報Ｌを第２演算部７５に渡すように構成することで、さまざまな利用制御を行うことが可能になる。

【０１４６】［実施例５］つぎに本発明の実施例５について説明する。実施例５は、衛星放送を利用してカプセル化されたコンテンツを配信して、サービスを提供する例である。ここで、カプセル化とは暗号化等を施すことによりコンテンツをそのままでは利用できないようにすることを指す。図１５に衛星放送を利用したサービス提供システムの概略図を示す。カプセル化されたコンテンツは衛星放送を利用して、各ユーザに配信される。ユーザは衛星電波を衛星アンテナで受信し受信機１００に入力する。受信機では本発明のサービス提供装置が実装してあり、検証が成功した場合にコンテンツを利用できるようになっている。

【０１４７】ここで提供されるコンテンツは、映画、音楽、テレビ番組、ソフトウエア、写真、文献、ニュース等さまざまなものが考えられる。それぞれのコンテンツは受信機１００に接続されたテレビ・ビデオ２００、オーディオ機器３００、コンピュータ（ＰＣ）４００等で利用される。ここでは、受信機１００とサービス利用機器が分割されている例について説明するが、受信機１００が内蔵されたサービス利用機器でも同様に説明できる。

【０１４８】カプセル化されたコンテンツの構造を図１６に示す。カプセル化されたコンテンツは、コンテンツヘッダと暗号化されたデータとに分類される。コンテンツヘッダはコンテンツの識別をするためのラベルと公開鍵（Ｅ，ｎ）および暗号化された復号鍵を有している。暗号化されたデータは前記の実施例で暗号化されたコンテンツ本体に相当する。

【０１４９】図１７は図１５における受信機１００の構成を具体的に示した例である。受信機１００の各回路はマイクロコンピュータによってコントロールされている。衛星アンテナからの衛星信号は、まず受信機１００のチューナ１０１に入力される。チューナ１０１は受信機１００のパネルもしくはリモコンによりユーザが選択したチャネルのデータを抽出する。誤り訂正回路／デス

クランブル回路１０２は、抽出されたデータをコンテンツとして復元し、データ・コントロール回路１０３に入力する。データ・コントロール回路１０３では、コンテンツがカプセル化されているかどうかをコンテンツラベルで識別し、コンテンツがカプセル化されていない場合は、そのまま出力側へ渡す。コンテンツがカプセル化されている場合には、コンテンツを検証／復号回路１０４に入力する。検証／復号回路１０４では、これまでの実施例で示した検証ルーチンにより正当性を検証することが可能であるが、実施例５では、別の方法を示して説明する。この方法の詳細については図１８を参照して説明する。なお、復号されたデータはデマルチプレクス回路１０５を介してビデオデコーダ１０６またはオーディオデコーダ１０７の送られて対応する信号として利用機器に供給される。

【０１５０】図１８に、実施例５の検証手順（プロトコル）を示す。実施例１と同様の機能を有する部分は同じ番号で示してある。

【０１５１】実施例５におけるアクセスチケットｔは式１４に基づいて生成されるデータである。

【０１５２】

【数１４】（１４）　　$t = D - F(n, e)$

上式中の記号はすべて整数であり、以下を表す。（実施例１の式参照）

ｎはＲＳＡ法数、即ち十分大きな二つの素数ｐ、ｑの積である（ｎ＝ｐｑ）。φ（ｎ）はｎのオイラー数、即ち、ｐ－１とｑ－１の積である（φ（ｎ）＝（ｐ－１）（ｑ－１））。ｅはユーザ固有情報を表し、ユーザ毎に異なる数で、ユーザを識別するために用いる。Ｄはアクセスチケット秘密鍵を表し、法数ｎのもとでのＲＳＡ秘密鍵であり、式２を満たす。ここで、ｇｃｄ（ｘ，ｙ）は二数ｘ、ｙの最大公約数を表す。

【０１５３】式（２）によって表現される性質は、式３を満たす数Ｅが存在することを保証する。Ｅをアクセスチケット公開鍵と呼ぶ。

【０１５４】二変数関数Ｆ（ｘ，ｙ）は関数値が衝突しにくい二変数関数であり、例えば前述の一方向性ハッシュ関数ｈを利用して式１５のように定めることができる。

【０１５５】

【数１５】

（１５）　　$F(x, y) = h(x \mid y)$

以下図を用いて、実施例５を詳細に説明する。図１７における検証／復号回路１０４は図１８では３８で示される。検証／復号回路３８は検証ルーチン１５と復号部６１とからなり、ＡＳＩＣ（ａｐｐｌｉｃａｔｉｏｎ ｓｐｅｃｉｆｉｃｉｎｔｅｇｒａｔｅｄ ｃｉｒｃｕｉｔ）等で実現されることで、復号の高速処理や検証ルーチンの安全性が保証される。もちろん検証／復号回路３８をソフトウエアプログラムで実現することも可能である。また、より安全性を高めるために、前述した耐タンパ特性を有するハードウエアで構成してもよい。検証／復号回路では、データ・コントロール回路より受け取ったカプセル化されたコンテンツをデータ分離部５６でコンテンツヘッダと暗号化されたデータとに分離し、公開鍵（Ｅ，ｎ）をアクセスチケット公開鍵記憶部５１に、暗号化された復号鍵K^Eを認証データ記憶部５２に、暗号化されたデータを復号部６１にそれぞれ格納する。そして検証／復号回路は内部の乱数生成部で乱数を生成し乱数記憶部５４に記憶する一方で、送信データ計算部において送信データＣを実施例１と同様に式５に基づいて計算する。

【０１５６】このようにして計算した送信データＣは、法数ｎと一緒に証明プログラムに送信される。

【０１５７】証明プログラムの第１演算部７３および証明データ生成部７６の演算はマイクロコンピュータで実行され、アクセスチケットはＥＰＲＯＭ（ｅｒａｓａｂｌｅｐｒｏｇｒａｍｍａｂｌｅ ｒｅａｄ ｏｎｌｙ ｍｅｍｏｒｙ）等に記憶されている。認証データは受信したｎを基にアクセスチケット記憶部７２から、対応するアクセスチケットｔを選択し、認証データ受信部７１から受け取ったＲＳＡ法数ｎのもとで、式１６を実行し中間情報Ｒ’を得る。

【０１５８】

【数１６】

（１６）　　$R' = C^t \mod n$

トークンはＩＣカードにより実現され、ユーザ固有情報記憶部７４および第２演算部７５を有し、マイクロコンピュータから認証用データを受け取って式１７を実行し差分情報Ｓを得る。

【０１５９】

【数１７】

（１７）　　$S = C^{F(n,e)} \mod n$

そして、証明プログラムの証明データ生成部７５は第１および第２演算部７３、７５から中間情報Ｒ’および差分情報Ｓを得て、式１８の計算を行い証明データＲを得る。

【０１６０】

【数１８】（１８）　　$R = R' S \mod n$

このようにして得られた証明データＲは、検証／復号回路の証明データ受信部５７に送信される。

【０１６１】検証ルーチン１５の乱数効果除去部５８は、データ受信部５７で受信した証明データＲを取得し、乱数記憶部５４に記憶されている乱数ｒとにより、式１９の計算を行い復号鍵Ｋを得る。

【０１６２】

【数１９】（１９）　　$K = R r^{-1} \mod n$

このときＫに冗長性をもたせ、その部分に特定の値を持たせておくことで、復号鍵Ｋが正しく復号されたかどうかを検証部５９で検証するようにしてもよい。得られた

復号鍵Ｋは復号部６１に入力され、復号部６１では暗号化されたデータを復号鍵Ｋを用いて復号しコンテンツとして出力する。

【０１６３】出力されたコンテンツは、デジタルデータとしてＰＣで利用されたり、映像情報やオーディオ情報として利用されたりする。

【０１６４】図１９に、本実施例のサービス提供装置の概観図を示す。図に示すようにサービス提供装置はテレビに接続されている。図には示してないがサービス提供装置は衛星アンテナに接続されており、衛星放送を受信する一方、モデムを通してネットワークに接続されており、衛星放送で受信したカプセル化されたコンテンツを利用するためのアクセスチケットを取得できるようになっている。図１９（ａ）に示すように、コンテンツが暗号化されている場合はトークンをサービス提供装置に挿入していない場合は、ユーザは映像を観ることができない。そこで、ユーザは正当なアクセスチケットを取得してサービス提供装置にトークンを挿入すると、図１９（ｂ）に示すように映像を見ることができるようになる。

【０１６５】このように、本発明では、コンテンツを１つの暗号鍵で暗号化して提供しているにもかかわらず、各ユーザ毎にカスタマイズされたアクセスチケットとユーザ固有情報を格納したトークンを両方有しないとサービスを利用することができないようになっている。従ってコンテンツのプロバイダ（提供者）は、コンテンツを暗号化して衛星放送のようなマスメディアを利用して提供することが可能であり、また、アクセスチケットとトークンとによりユーザごとの確実な利用管理を行うことが可能である。

【０１６６】［実施例６］つぎに本発明の実施例６について説明する。上記はコンテンツごとにカプセル化した場合について記述したが、これ以外の応用例として、衛星放送の放送チャネルについては同じ暗号化を施し、視聴時間を管理することでコンテンツの利用を制限したい場合などがある。このようなサービスはアクセスチケットを式２０で表現することで実現される。

【０１６７】

【数２０】（２０）　　$t = D - F(n, e, L)$

ここで、Ｌは利用制御情報であり、利用期限を表す。三変数関数Ｆ（ｘ，ｙ，ｚ）は関数値が衝突しにくい三変数関数であり、例えば前述の一方向性ハッシュ関数ｈを利用して式２１のように定めることができる。

【０１６８】

【数２１】

（２１）　　$F(x, y, z) = h(x \mid y \mid z)$

図２０に利用制御情報の構成例を示す。図に示すとおり利用制御情報Ｌは利用開始時刻、利用終了時刻および利用料金とで構成される。利用料金はトークンがプリペイド機能を有する場合にのみ必要で、プリペイド機能を使わない場合は省略することができる。図２１に利用制御情報Ｌを用いた場合の検証プロトコルを示す。ここで図１８と同様の機能のものは同じ番号で示してある。

【０１６９】以下、図を用いて実施例６を詳細に説明する。検証／復号回路では、データ・コントロール回路より受け取ったカプセル化されたコンテンツをデータ分離部５６でコンテンツヘッダと暗号化されたデータとに分離し、公開鍵（Ｅ，ｎ）をアクセスチケット公開鍵記憶部５１に、暗号化された復号鍵K^Eを認証データ記憶部５２に、暗号化されたデータを復号部６１にそれぞれ格納する。そして検証／復号回路は内部の乱数生成部で乱数を生成し乱数記憶部５４に記憶する一方で、送信データ計算部において送信データＣを式１５に基づいて計算する。

【０１７０】このようにして計算した送信データＣは、法数ｎと一緒に証明プログラムに送信される。

【０１７１】証明プログラムの第１演算部７３および証明データ生成部７６の演算はマイクロコンピュータで実行され、アクセスチケットはＥＰＲＯＭ（ｅｒａｓａｂｌｅｐｒｏｇｒａｍｍａｂｌｅ　ｒｅａｄ　ｏｎｌｙ　ｍｅｍｏｒｙ）等に記憶されている。認証データは受信したｎを基にアクセスチケット記憶部７２から、対応するアクセスチケットｔと利用制御情報Ｌを選択し、認証データ受信部７１から受け取ったＲＳＡ法数ｎのもとで、式１６を実行し中間情報Ｒ’を得る。

【０１７２】トークンは、ユーザ固有情報記憶部７４、第２演算部７５を有し、さらに、プリペイド度数とトークン時刻データを有している。トークンは、マイクロコンピュータから認証用データと利用制御情報Ｌを受け取り、利用制御情報中の有効期限がトークン時刻と矛盾しないかどうかを検証する。すなわち、利用開始時刻≦トークン時刻≦利用終了時刻となっている場合に検証が成功したとみなされる。有効期限の検証に成功したら、トークンの度数が利用制御情報Ｌ内の利用度数以上残っていることを確認し、残っていればトークンの度数から利用制御情報Ｌ内の利用度数分を減算する。有効期限の検証に失敗した場合と、度数が足りない場合は処理を行わずエラーを返す。上記の検証が成功した場合は、式２２を実行し差分情報Ｓを得る。

【０１７３】

【数２２】

（２２）　　$S = C^{F(n, e, L)} \mod n$

そして、証明プログラムの証明データ生成部７５は第１および第２演算部７３、７５から中間情報Ｒ’および差分情報Ｓを得て、式１８の計算を行い証明データＲを得る。このようにして得られた証明データＲは、検証／復号回路の証明データ受信部５７に送信される。

【０１７４】検証ルーチン１５の乱数効果除去部５８は、データ受信部５７で受信した証明データＲを取得し、乱数記憶部５４に記憶されている乱数ｒとにより、

式１９の計算を行い復号鍵Ｋを得る。ここで、もしトークンで用いた利用制御情報Ｌが改ざんされていた場合は、正確な復号鍵を取り出すことができない。このときＫに冗長性をもたせ、その部分に特定の値を持たせておくことで、復号鍵Ｋが正しく復号されたかどうかを検証部５９で検証するようにしてもよい。得られた復号鍵Ｋは復号部６１に入力され、復号部６１では暗号化されたデータを復号鍵Ｋを用いて復号しコンテンツとして出力する。

【０１７５】出力されたコンテンツは、デジタルデータとしてＰＣで利用されたり、映像情報やオーディオ情報として利用されたりする。

【０１７６】この実施例では、トークンに時刻を持たせているが、ＩＣカードを用いる場合は内部に時計が無いので、トークン時刻の正当性を保証することが必要となる。

【０１７７】このようにすることで、ユーザはアクセスチケットを利用制御情報中の有効期限内でないと利用できず、１つのチャネルのコンテンツが同じ暗号鍵で暗号化してあったとしても、時間毎に利用権を設定することができ、ペイパービュー等の機能を実現することも可能である。

【０１７８】なお、本発明は上述の実施例に限定されるものではなく、例えば、コンテンツの利用は、種々の記録媒体、通信媒体、放送媒体を介して行える。インターネット、衛星放送の他に、種々の通信媒体、放送媒体を利用する場合に適用できる。例えば、通常の電話網、データ通信網、ＴＣＰ／ＩＰ接続による通信カラオケのサービスの提供にも適用できる。

【０１７９】

【発明の効果】以上説明したように、本発明によれば、証明用補助データ（アクセスチケット）を導入することにより、アクセス資格認証の特徴情報とユーザ固有情報とを独立させることができ、従って、プロテクト側も、ユーザ側も１つの固有情報を準備しておけば済む。アクセスチケットは、特定のユーザ固有情報とアクセス資格認証の特徴情報とに基づいて計算されるデータであり、またユーザ固有情報を知らずにアクセスチケットからアクセス資格認証の特徴情報を計算することは少なくとも計算量適に不可能である。そして、ユーザ固有情報とアクセスチケットの正しく組み合わされた場合にのみ、サービスを提供（コンテンツを復号）するので、ユーザは予めユーザ固有情報を所持し、サービス提供者はユーザが所持するユーザ固有情報とは独立にアクセス資格認証の特徴情報を用意することができる。従って、例えばコンテンツを１つの暗号鍵で暗号化した場合でも、所望のユーザだけにアクセス権を設定することが可能となり、暗号化したコンテンツをユーザ毎に用意する必要が無くなる。

【図面の簡単な説明】

【図１】　本発明の原理的な構成例を示すブロック図である。

【図２】　実施例１の構成例の概要を示すブロック図である。

【図３】　実施例１のユーザが用いる計算機の概略図である。

【図４】　実施例１の構成例の詳細なブロック図である。

【図５】　実施例１の暗号化されたコンテンツの構成例１である。

【図６】　実施例１の暗号化されたコンテンツの構成例２である。

【図７】　実施例１の暗号化されたコンテンツの構成例３である。

【図８】　実施例１の検証部における処理の構成例である。

【図９】　実施例１の検証部における処理の構成例である。

【図１０】　実施例１の検証部における処理の構成例である。

【図１１】　実施例１の検証部における処理の構成例である。

【図１２】　実施例２の構成例の詳細なブロック図である。

【図１３】　実施例３の構成例の詳細なブロック図である。

【図１４】　実施例４の構成例の詳細なブロック図である。

【図１５】　実施例５の概略図である。

【図１６】　実施例５のカプセル化されたコンテンツの構成図である。

【図１７】　実施例５の構成例の詳細なブロック図である。

【図１８】　実施例５の構成例の詳細なブロック図である。

【図１９】　実施例５の構成例の図である。

【図２０】　実施例６の利用制御情報の構成図である。

【図２１】　実施例６の構成例の詳細なブロック図である。

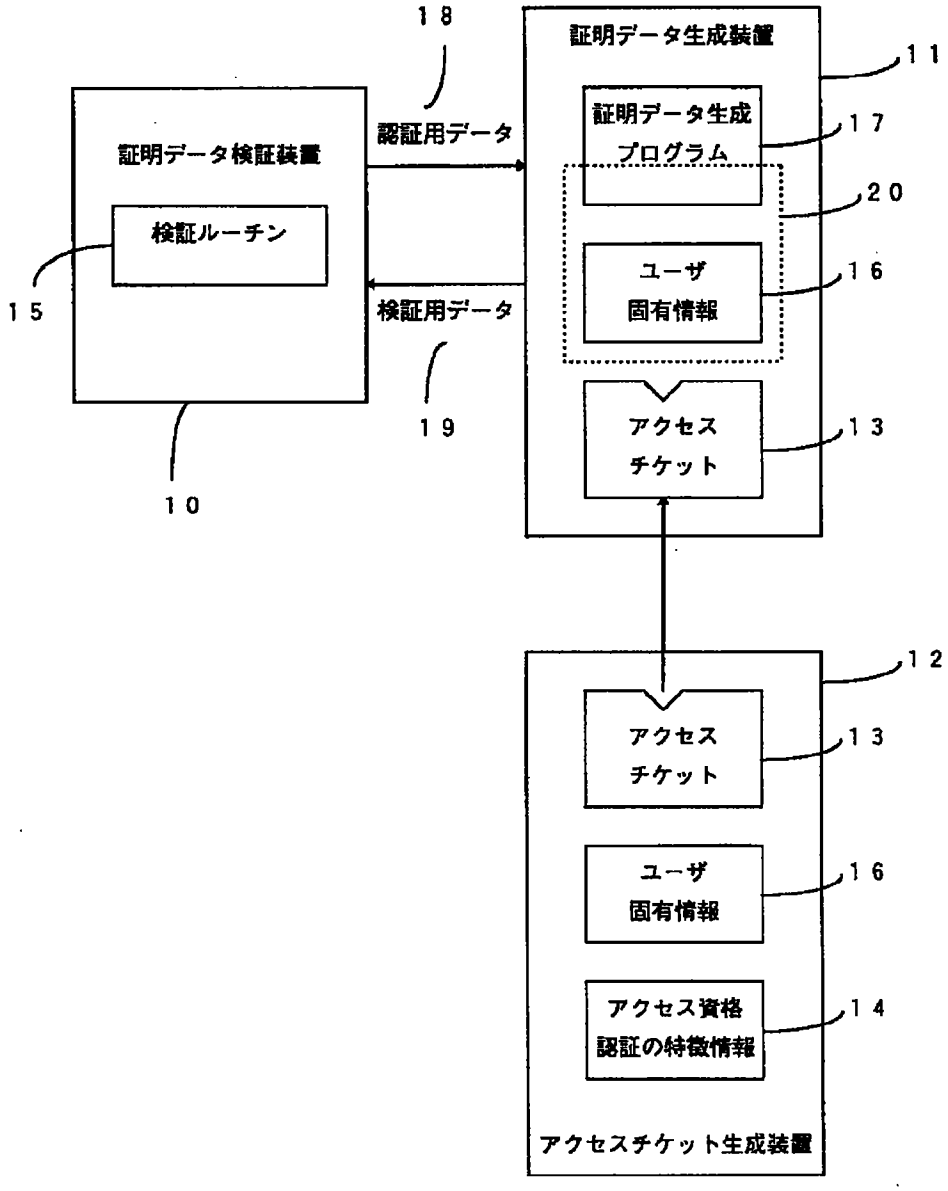
【符号の説明】

１０　証明データ検証装置
１１　証明データ生成装置
１２　アクセスチケット生成装置
１３　アクセスチケット（証明用補助データ）
１４　アクセス資格認証の特徴情報
１５　検証ルーチン
１６　ユーザ固有情報
１７　証明データ生成プログラム
１８　認証用データ
１９　証明データ

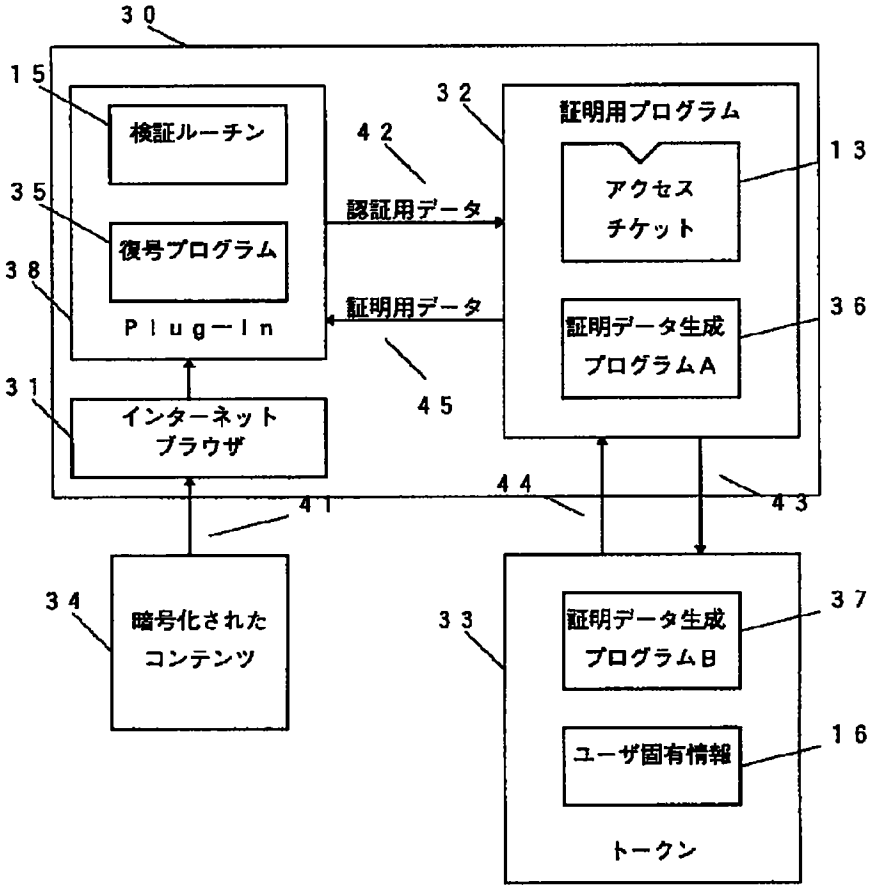
35　　36

２０　耐タンパー装置
３０　計算機
３１　インターネットブラウザ
３２　証明用プログラム
＊３３　トークン
３４　コンテンツ
３５　復号プログラム
＊　３８　プラグイン（プラグイン・モジュール）

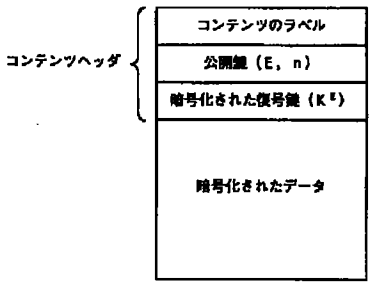
【図１】



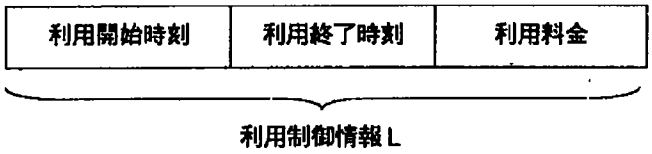
【図２】



【図１４】

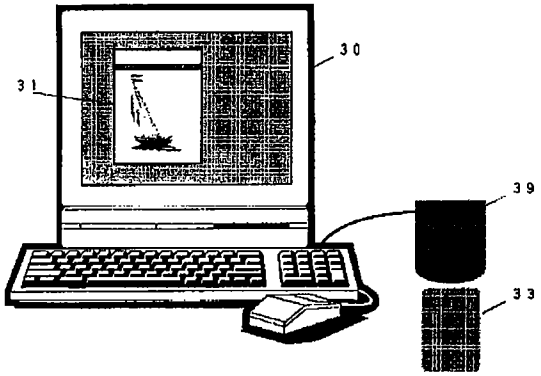


【図１８】

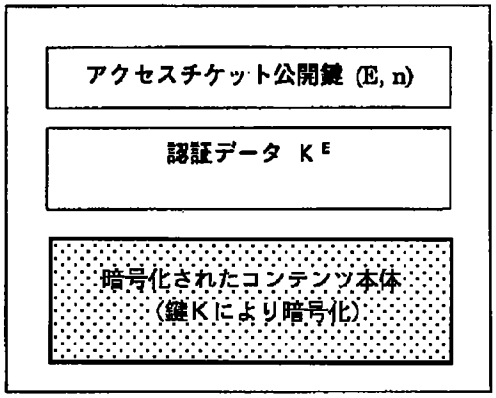


利用制御情報の構成図

【図３】

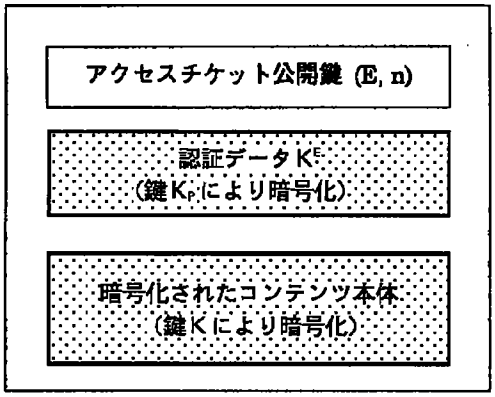


【図５】



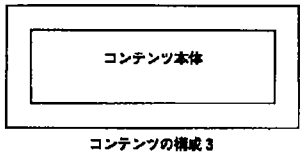
暗号化されたコンテンツの構成１

【図６】



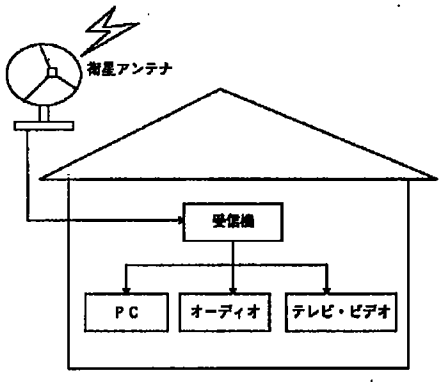
暗号化されたコンテンツの構成２

【図７】

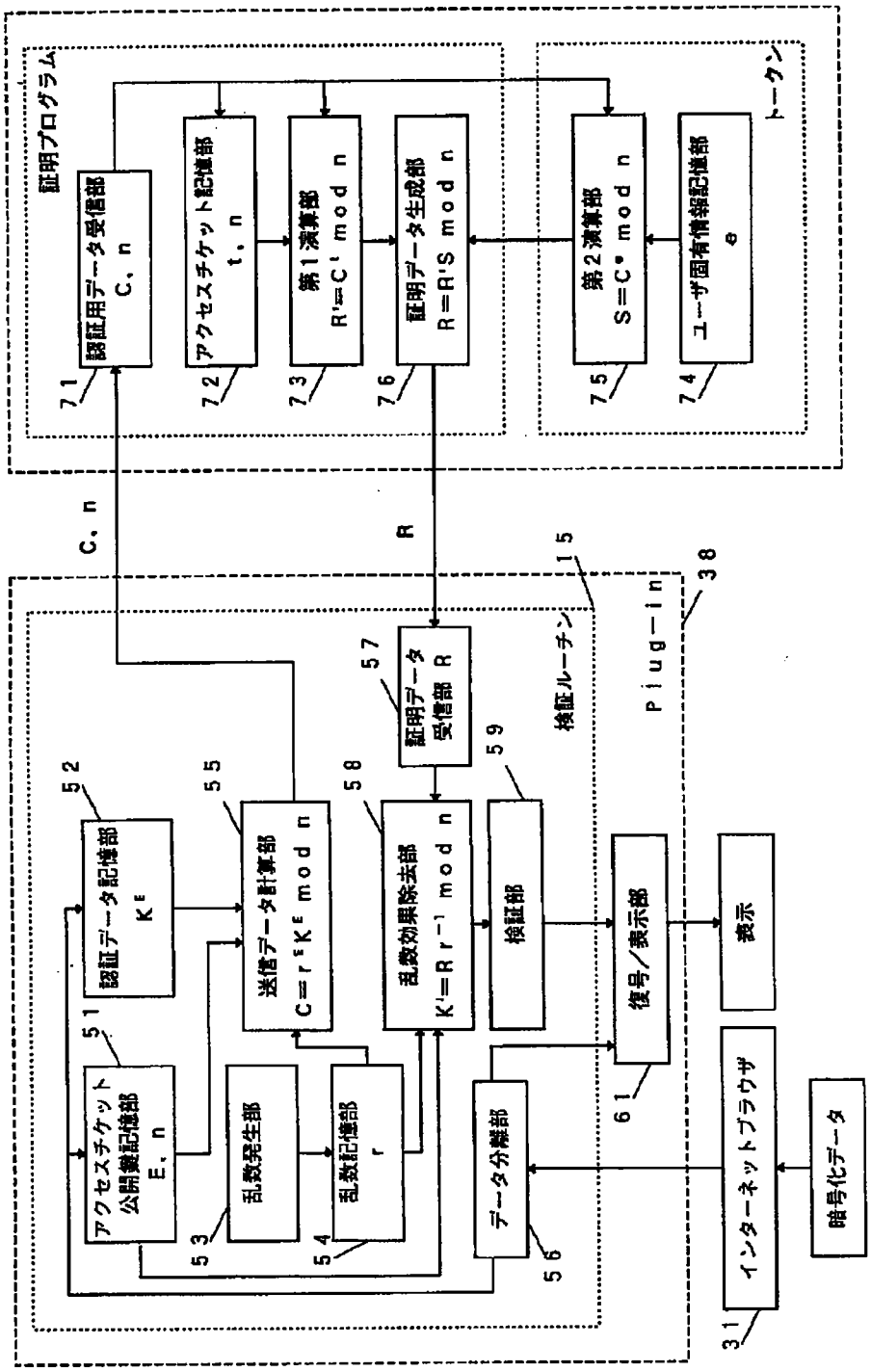


コンテンツの構成３

【図１３】

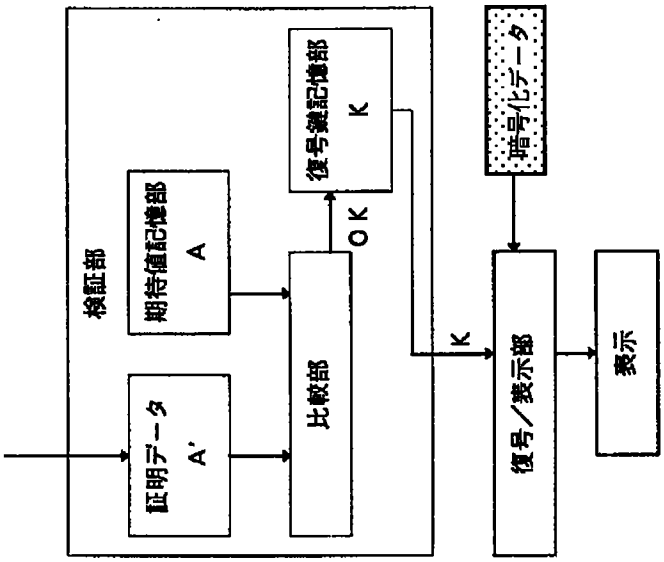


【図４】

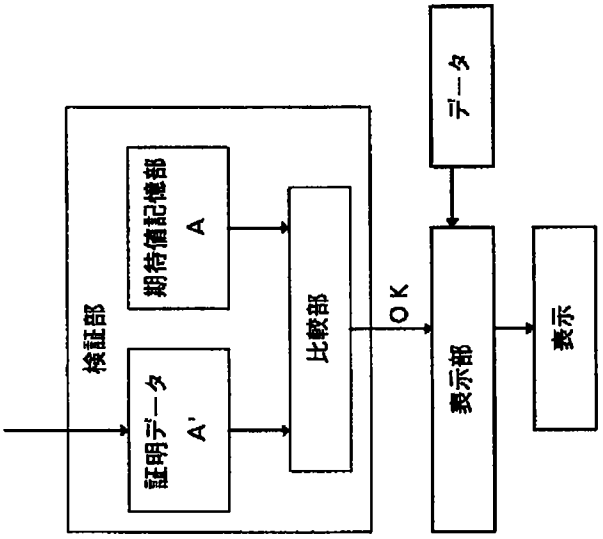


第１の実施例の詳細公構成例

【図８】

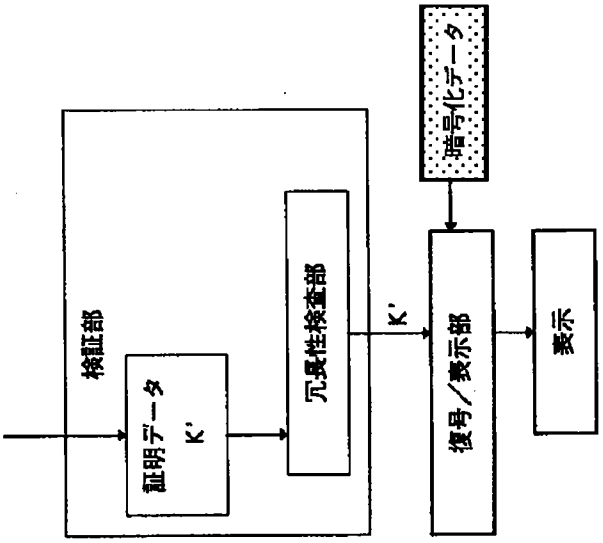


(b) 検証部の構成２

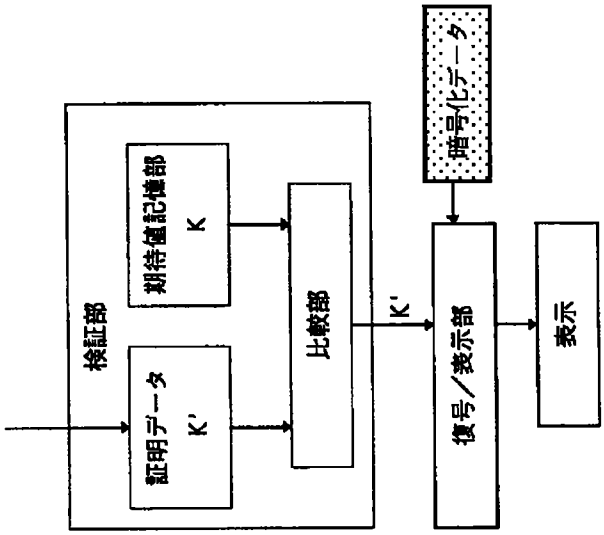


(a) 検証部の構成１

【図９】

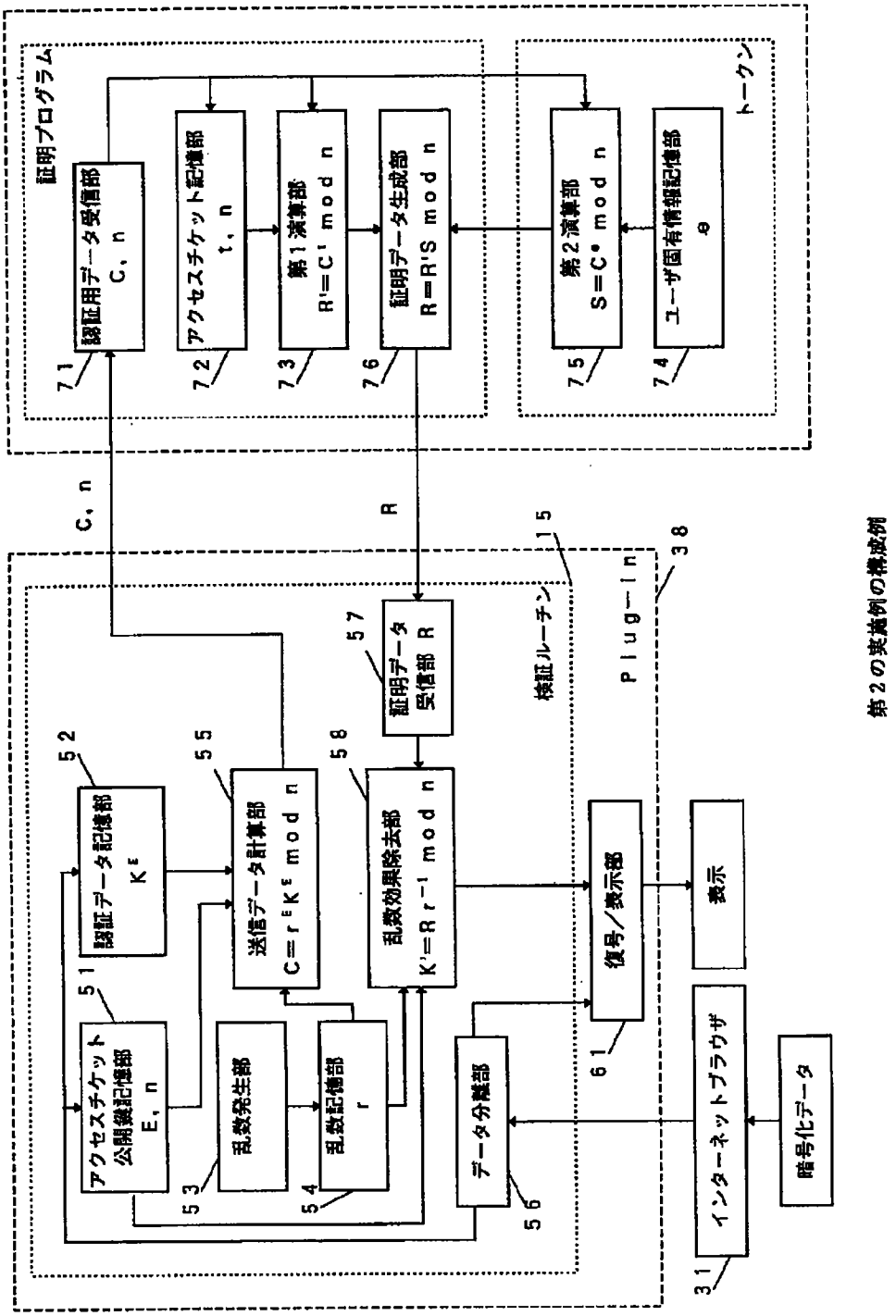


(d) 検証部の構成４



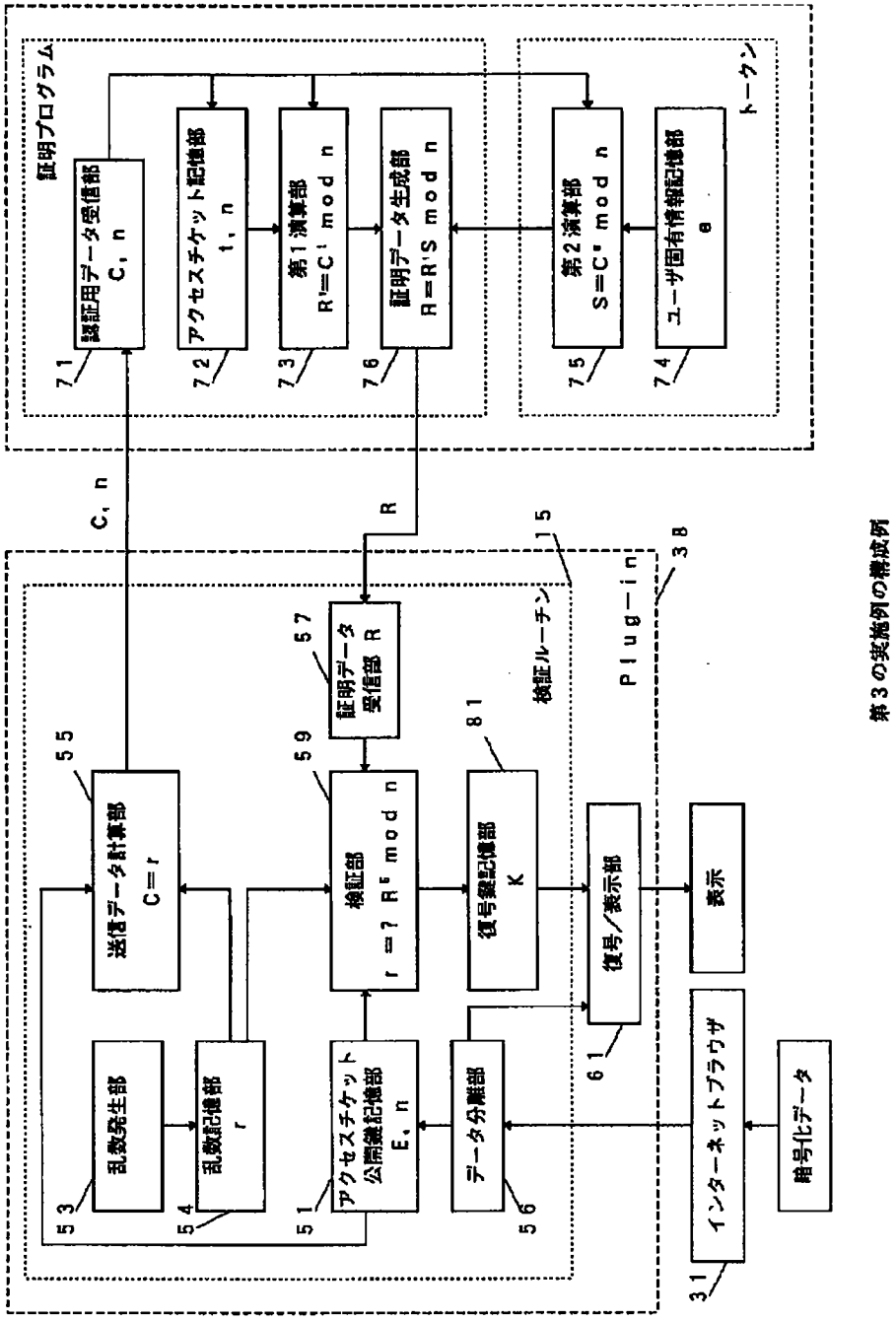
(c) 検証部の構成３

【図１０】



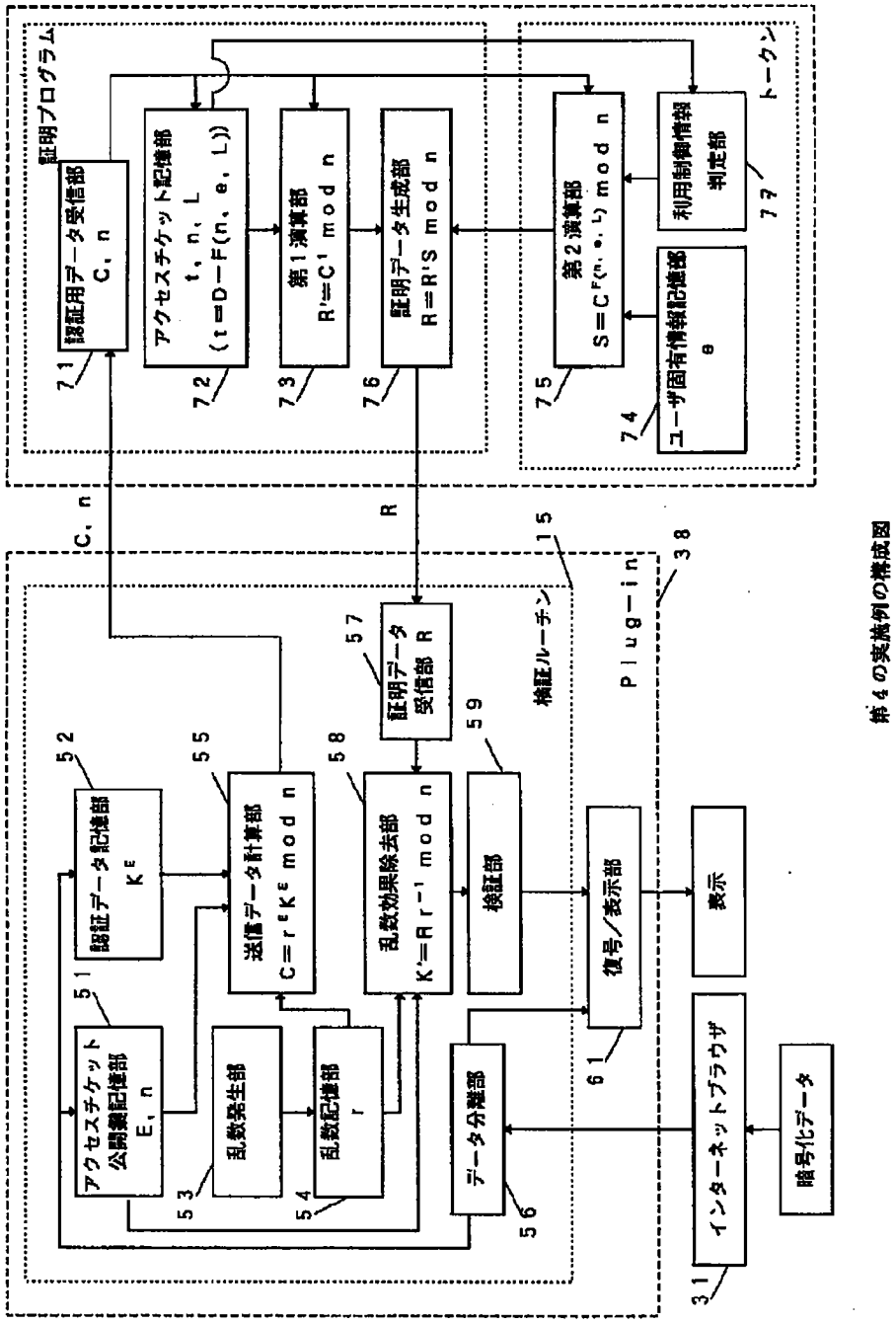
第２の実施例の構成例

【図１１】



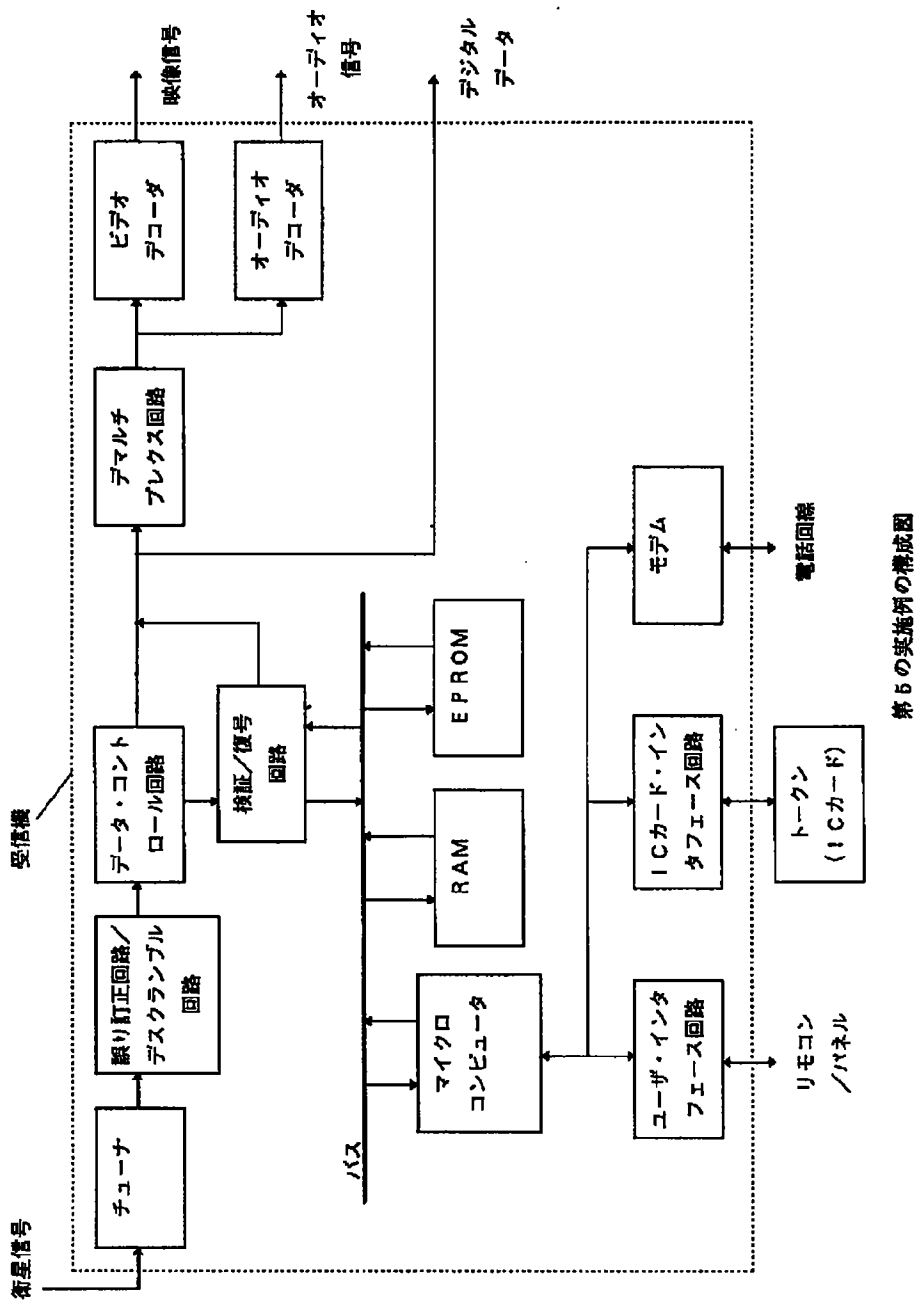
第３の実施例の構成例

【図１２】



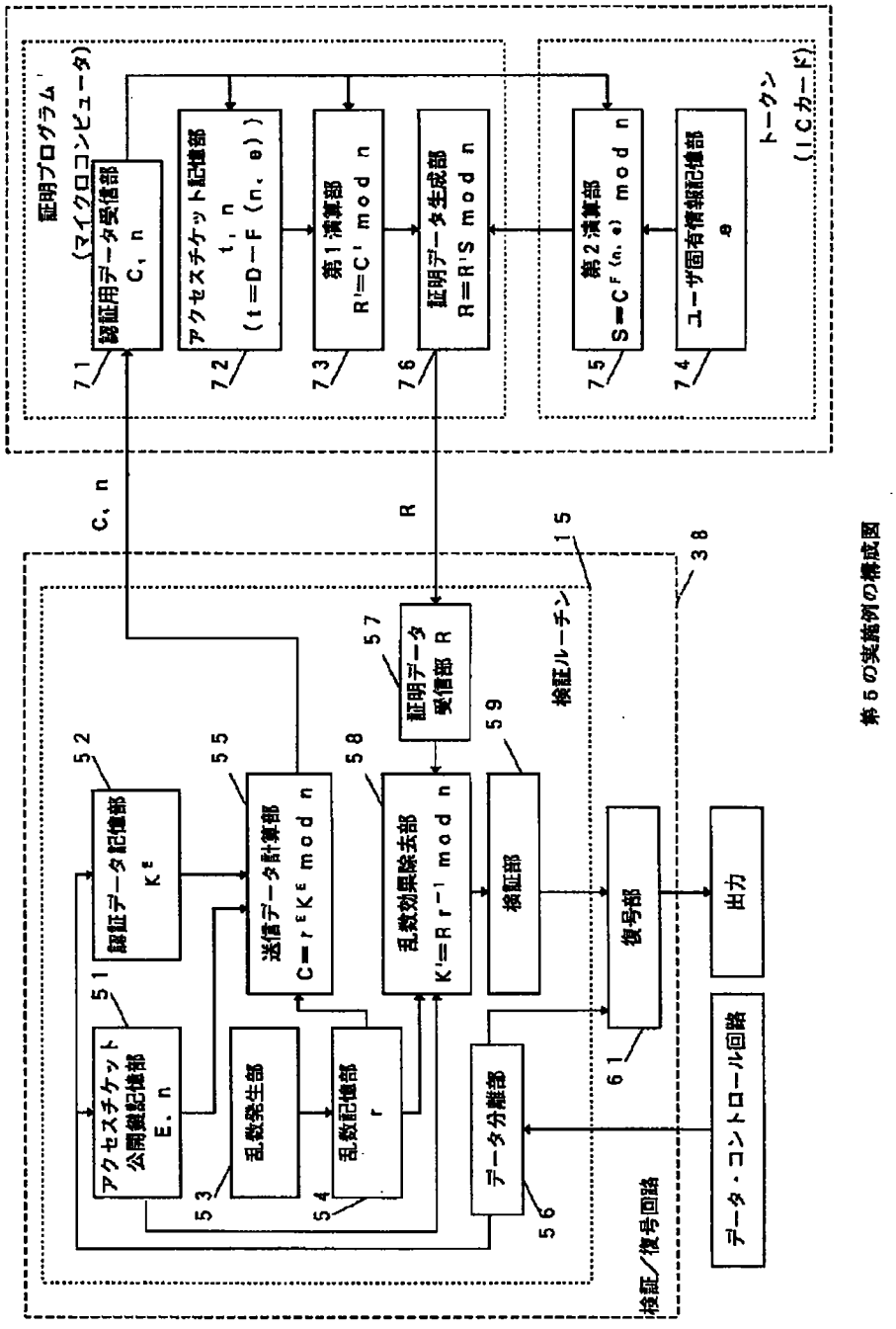
第４の実施例の構成図

【図１５】



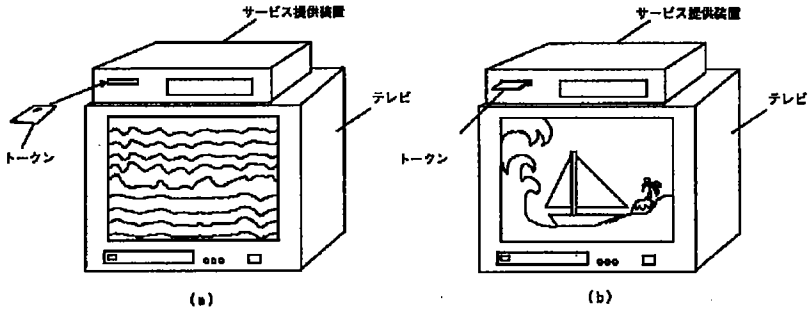
第５の実施例の構成図

【図１６】

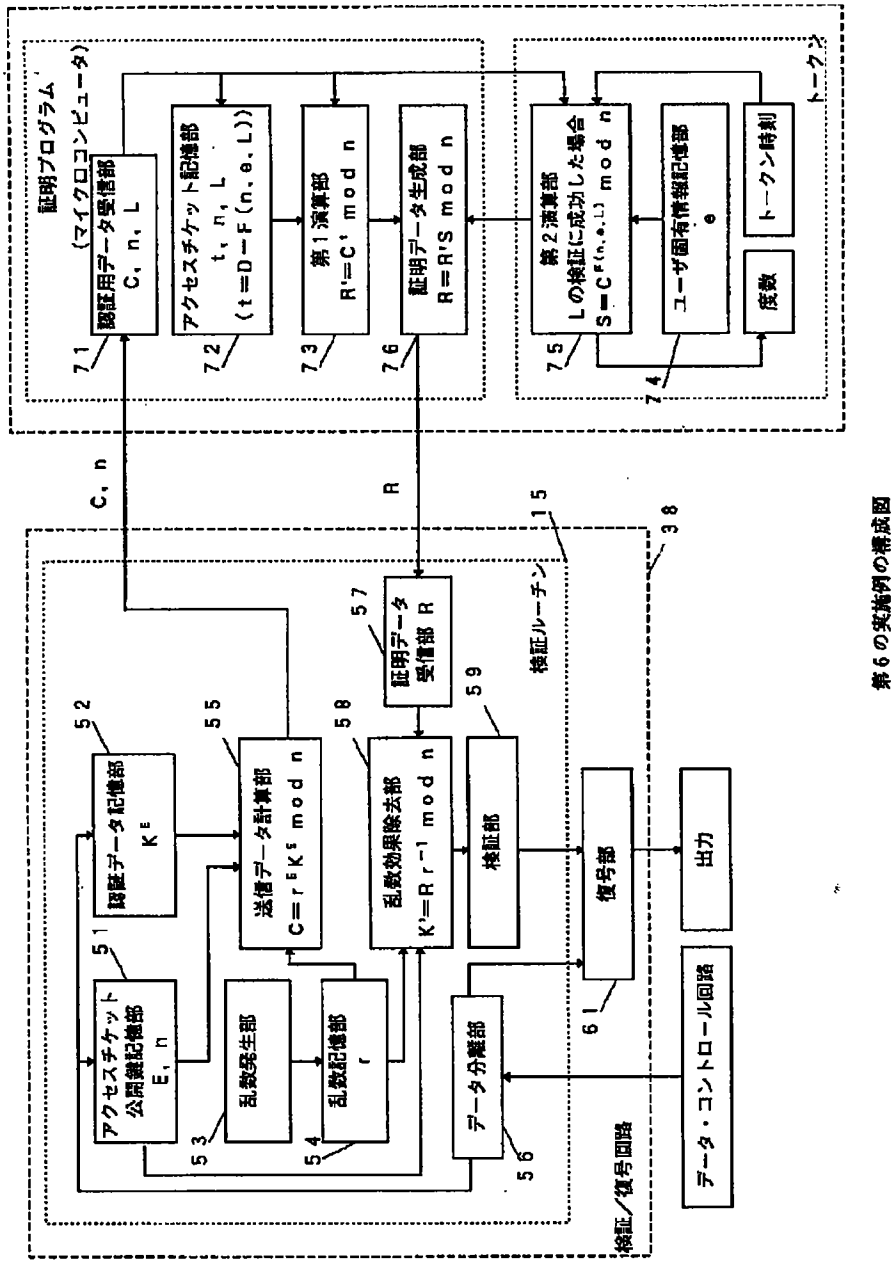


第６の実施例の構成図

【図１７】



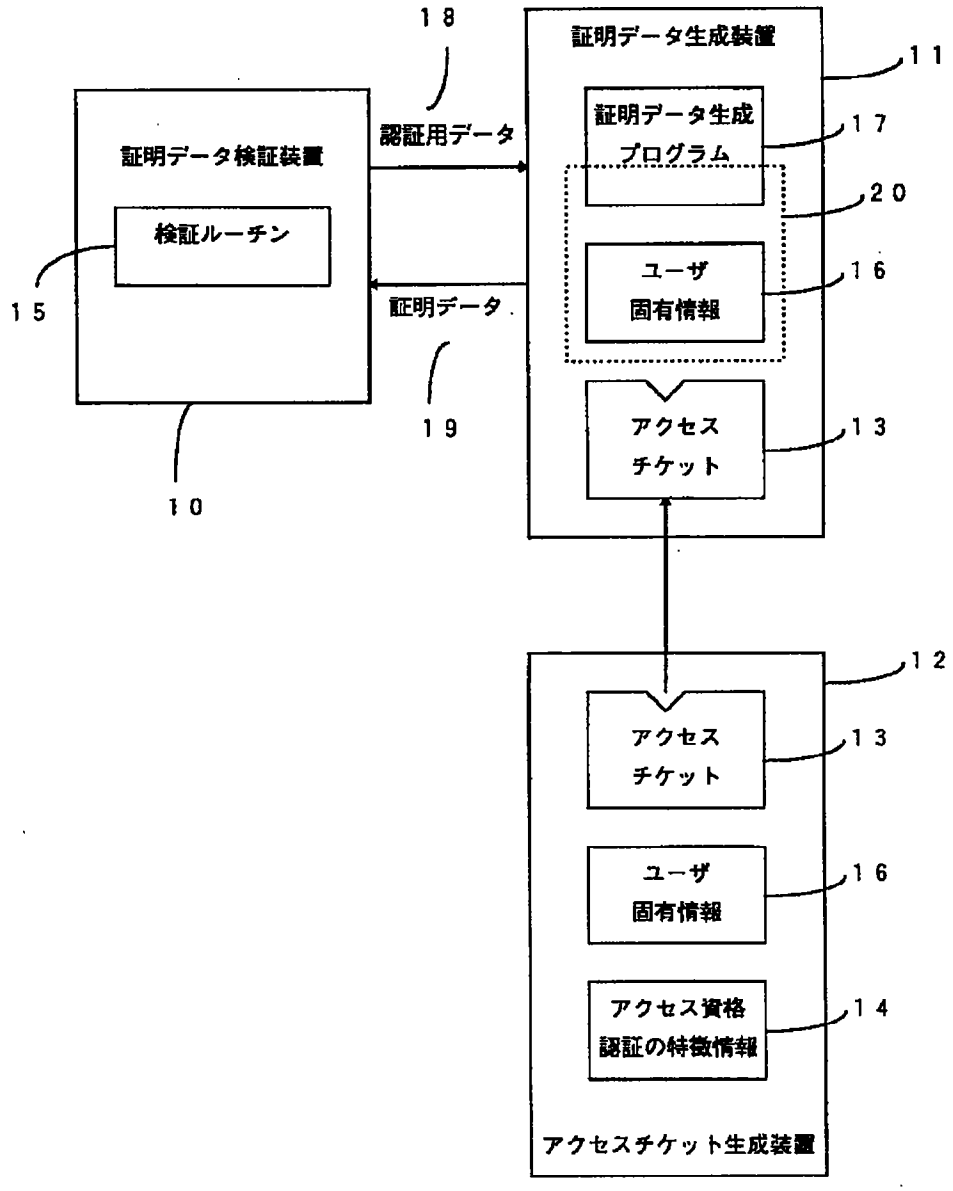
【図１９】



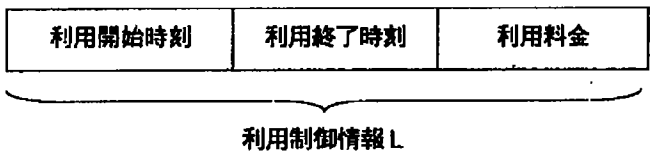
第６の実施例の構成図

【手続補正書】
【提出日】平成９年１０月２９日
【手続補正１】
【補正対象書類名】図面
【補正対象項目名】全図
【補正方法】変更
【補正内容】

【図１】

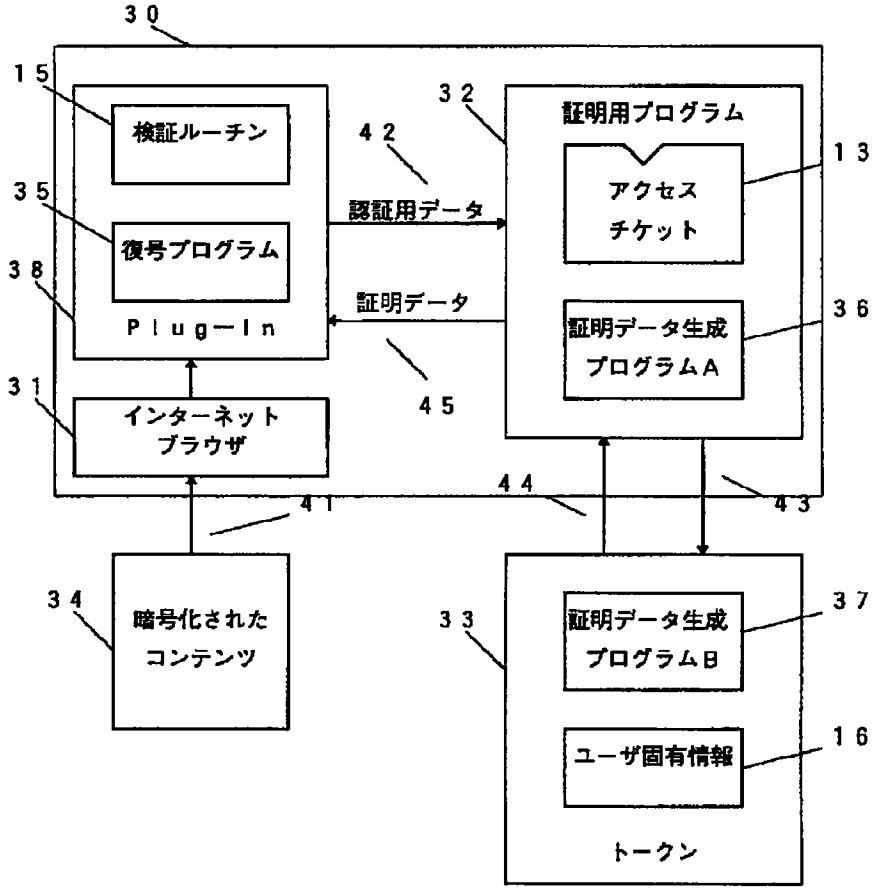


【図２０】

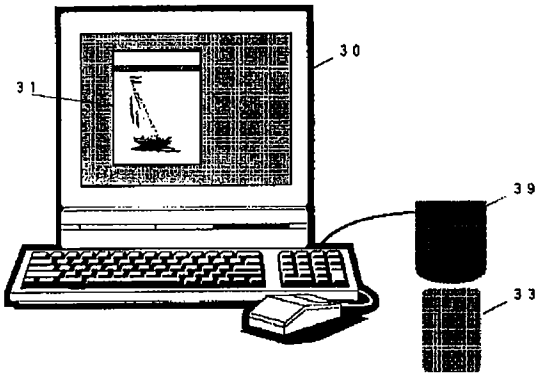


利用制御情報の構成図

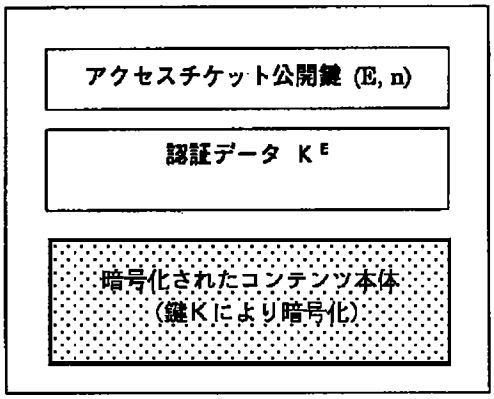
【図２】


３０
１５
検証ルーチン
３５
復号プログラム
３８
Ｐｌｕｇ－Ｉｎ
３１
インターネット
ブラウザ
３４
暗号化された
コンテンツ
４２
認証用データ
証明データ
４５
４１
４４
４３
３２
証明用プログラム
アクセス
チケット
１３
証明データ生成
プログラムＡ
３６
３３
証明データ生成
プログラムＢ
３７
ユーザ固有情報
１６
トークン

【図３】

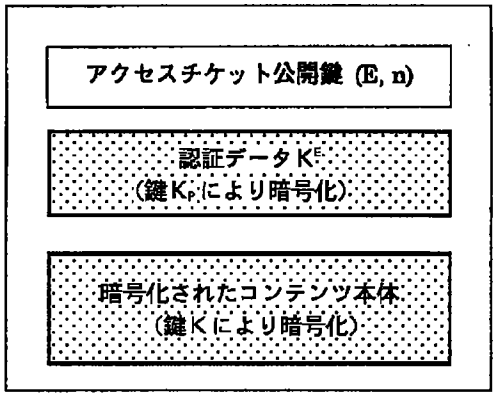


【図５】



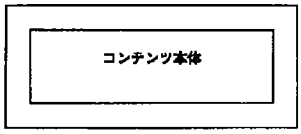
暗号化されたコンテンツの構成１

【図６】



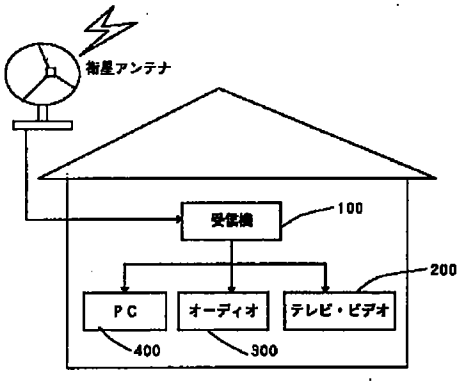
暗号化されたコンテンツの構成２

【図７】



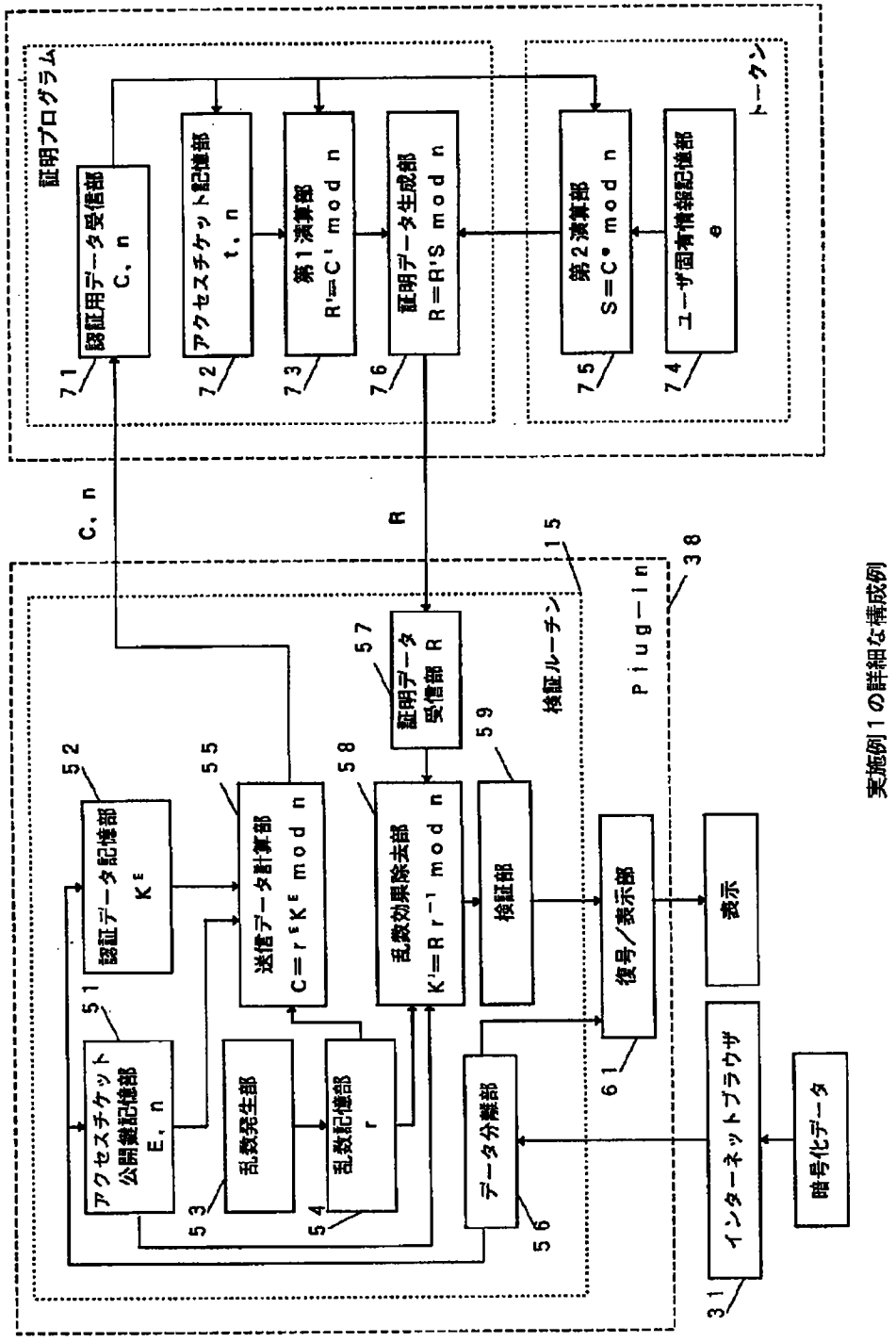
コンテンツの構成３

【図１５】



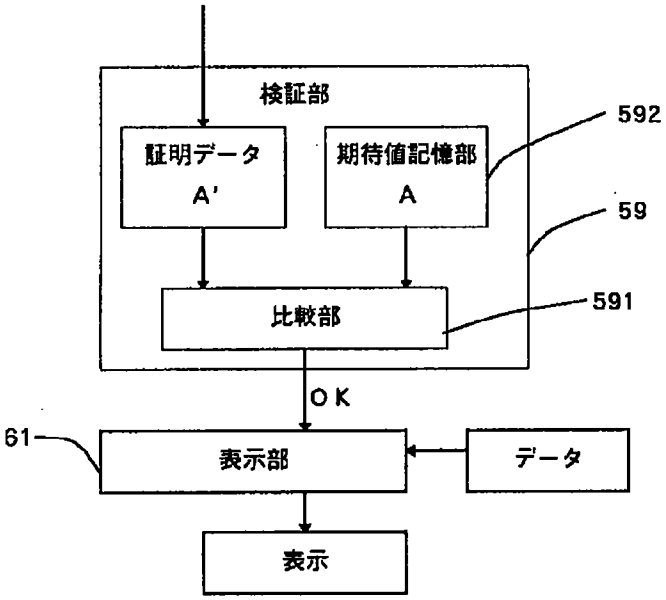
実施例５の説明図

【図４】



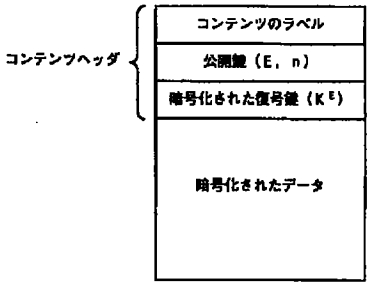
実施例１の詳細な構成例

【図８】



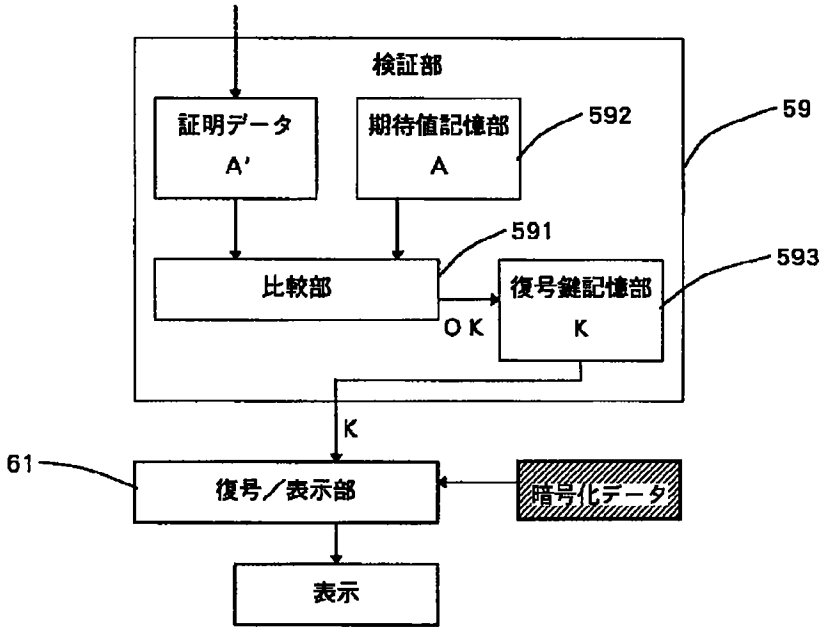
検証部の構成１

【図１６】



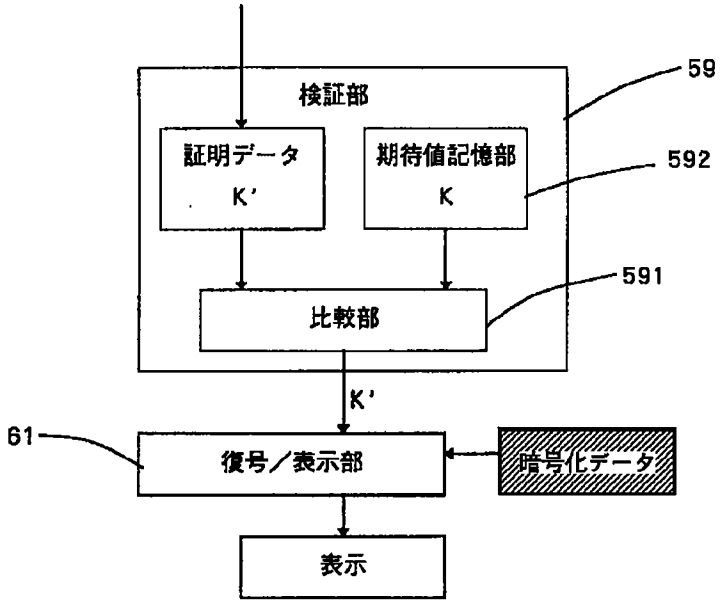
カプセル化されたコンテンツの構成図

【図９】



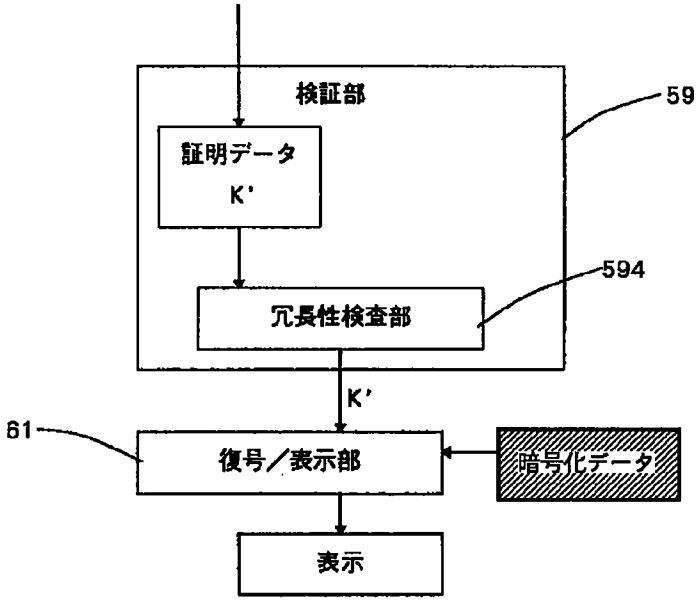
検証部の構成２

【図１０】



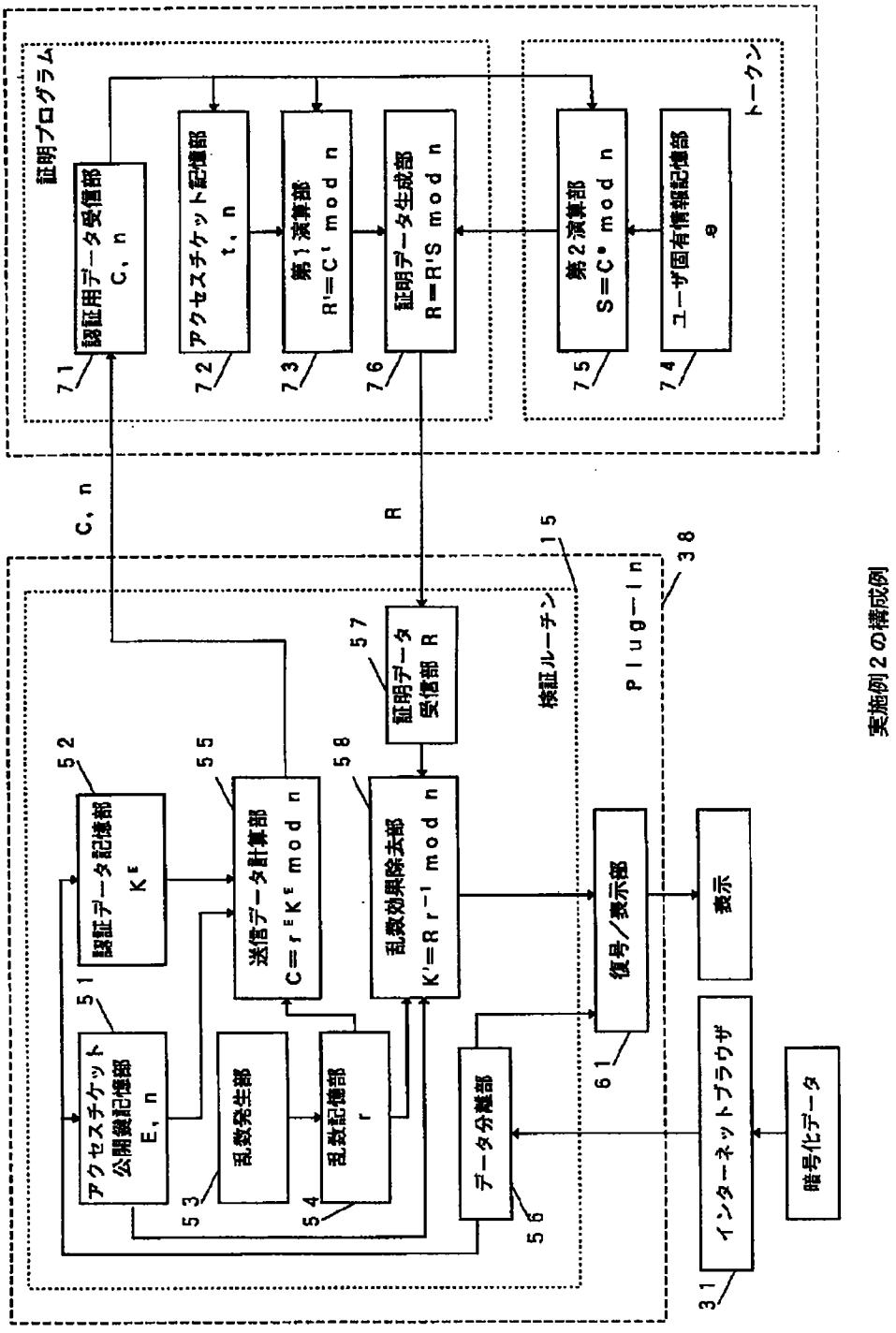
検証部の構成３

【図１１】



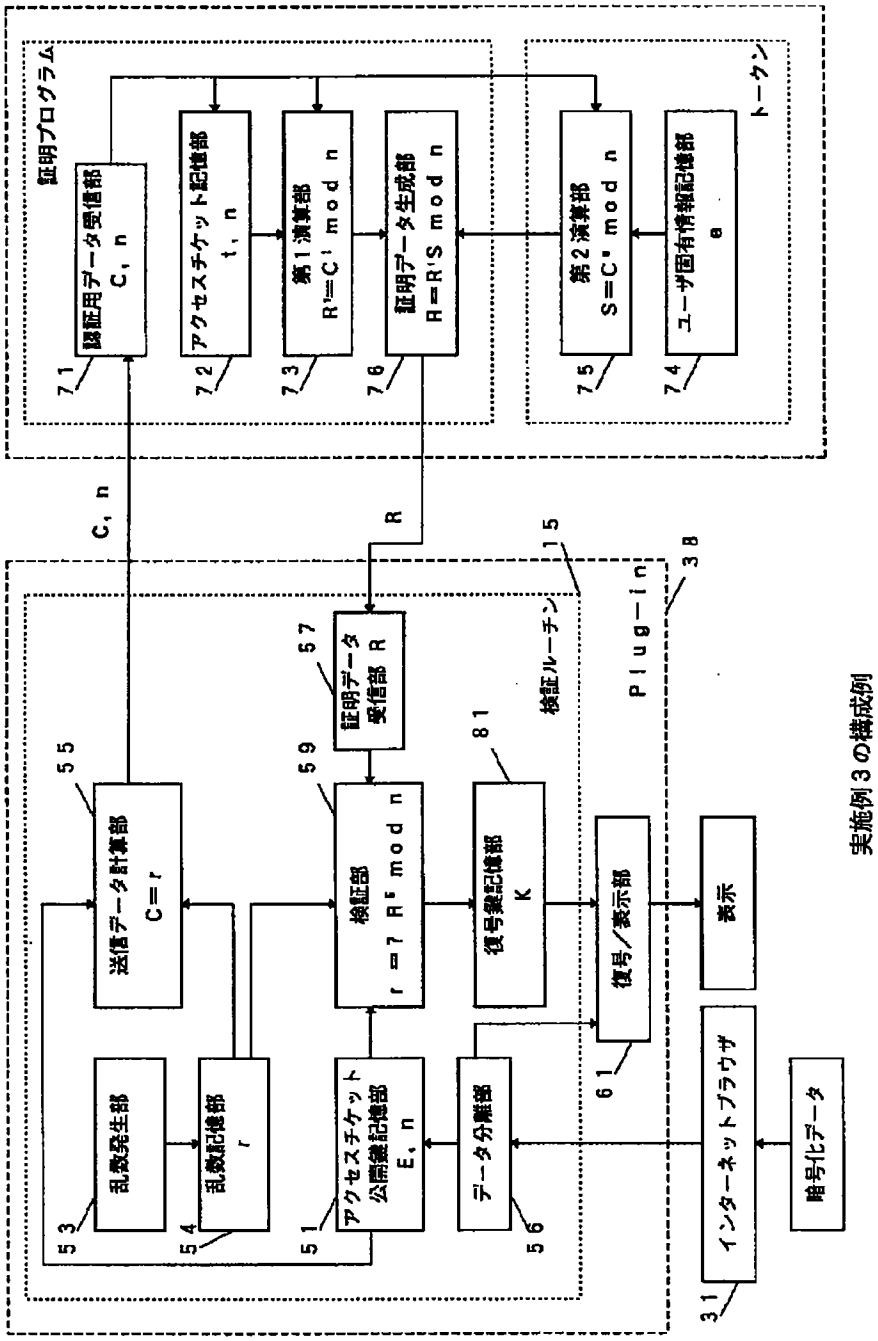
検証部の構成４

【図１２】



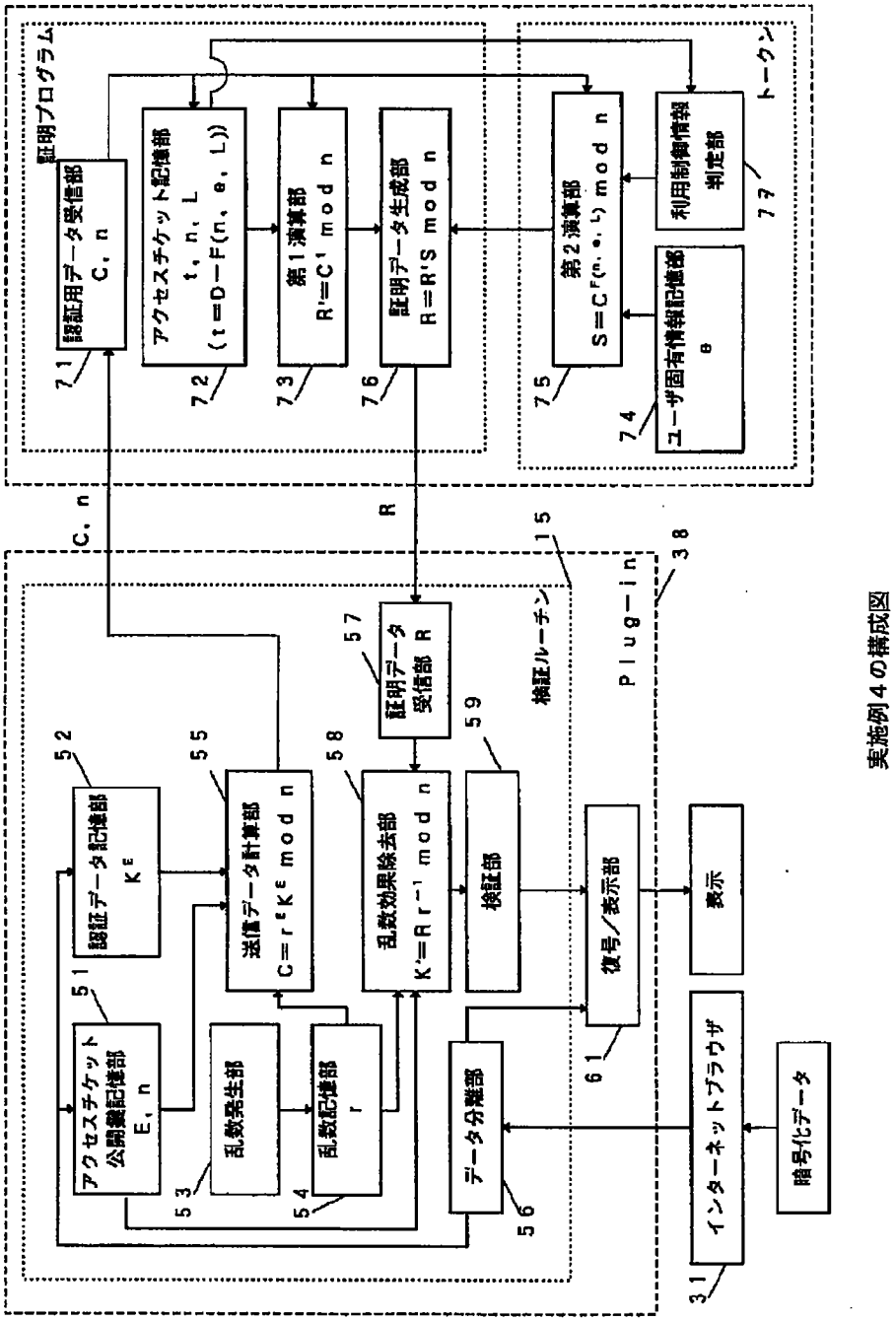
実施例２の構成例

【図１３】



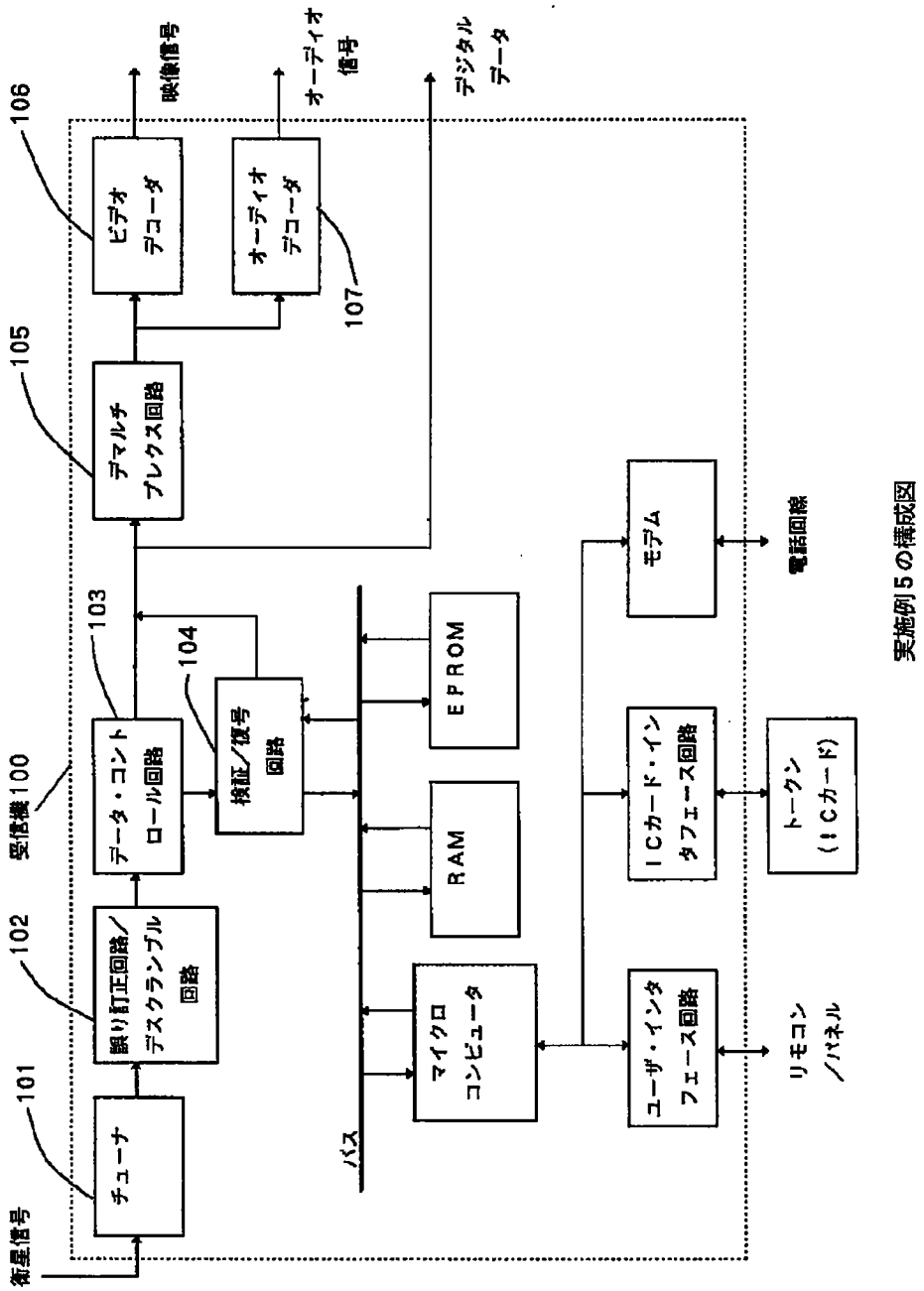
実施例３の構成例

【図１４】



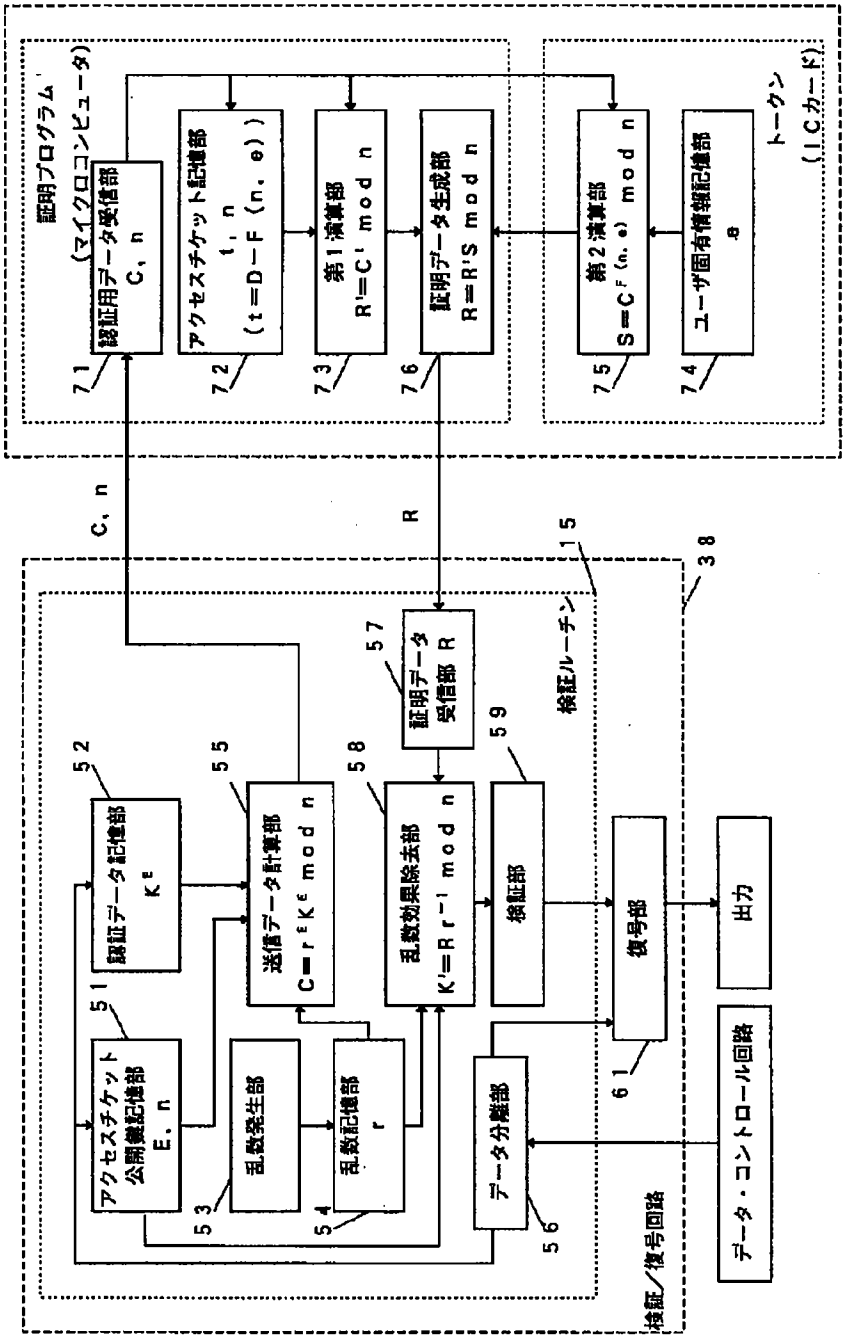
実施例４の構成図

【図１７】



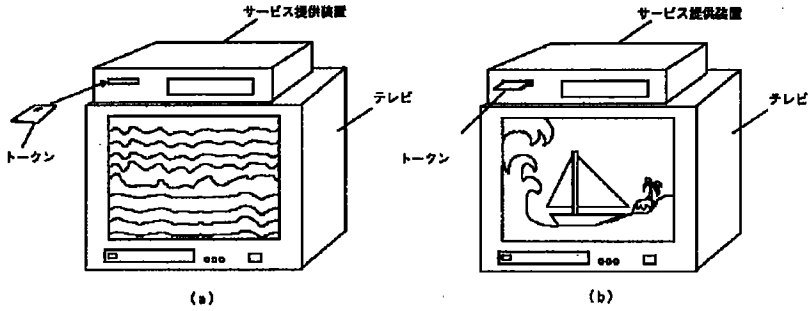
実施例５の構成図

【図１８】

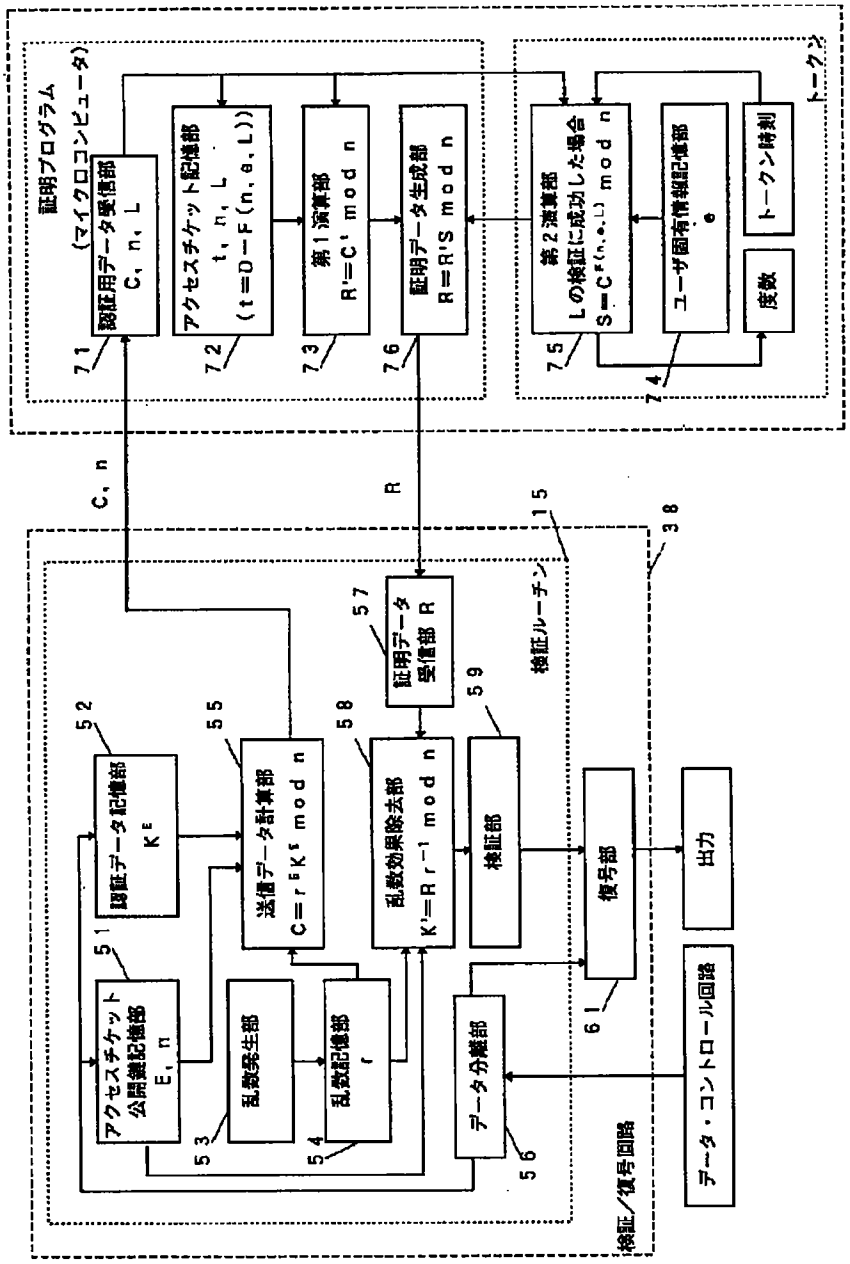


実施例５の構成図

【図１９】



【図２１】



実施例６の構成図